

La inteligencia artificial en la prevención e investigación del delito

Artificial Intelligence in the prevention and investigation of crime

Susana Jiménez López

Investigadora predoctoral, Universitat de Lleida

sjl4@alumnes.udl.cat

Andrea Planchadell Gargallo

Catedrática de Derecho Procesal, Universitat Jaume I

planchad@uji.es

<https://orcid.org/0000-0002-0448-0326>

Carolina Villacampa Estiarte

Catedrática de Derecho Penal, Universitat de Lleida

carolina.villacampa@udl.cat

<https://orcid.org/0000-0002-1791-8788>

Fecha de recepción: 28/09/24

Fecha de aceptación: 24/10/25

Resumen

En este trabajo se aborda el uso de la Inteligencia Artificial (IA) en la lucha contra el crimen. El objetivo principal es analizar si es posible una aplicación ética de la IA que respete los derechos fundamentales en la prevención e investigación del delito. Los resultados indican que la IA puede comportar no solo una importante intromisión en la privacidad de las personas, sino también un aumento de las discriminaciones y desigualdades sociales. Por lo que se concluye con la necesidad de que las Administraciones Públicas recuperen la “soberanía digital”, como garantes de los derechos fundamentales en la prevención e investigación criminal. Asimismo, el estudio pone de relieve la urgencia de establecer una regulación normativa con consenso a nivel global para evitar los “ciberparaísos” y velar porque el uso de la IA no suponga una laxitud de las garantías de los derechos de las personas, ni antes, ni después, de la comisión de un hecho delictivo.

Palabras clave: Inteligencia Artificial, prevención del delito, investigación criminal, sesgos algorítmicos, derechos fundamentales.

Abstract

The following paper tackles the use of Artificial Intelligence (AI) in the struggle against crime. The paramount aim is to analyse whether an ethical application of AI that respects fundamental rights in crime prevention and investigation is possible. The results prove that AI can lead not only to significant intrusions into citizens' privacy, but also to increasing discrimination and social inequality. Hence, the reassertion of “digital

sovereignty” by public administrations as the guarantors of fundamental rights in criminal prevention and investigation is needed. In this line, the research highlights the urgency for establishing a normative regulation with global consensus in order to avoid “cyberparadises” while ensuring that the use of AI does not lead to a lax attitude towards citizens’ rights, either before or after a criminal act is committed.

Keywords: Artificial Intelligence, crime prevention, crime investigation, algorithmic bias, fundamental rights.

Introducción

La irrupción de la IA, especialmente de los sistemas generativos como ChatGPT, y su velocidad de desarrollo sin precedentes ha impactado de manera significativa en la sociedad contemporánea. Los laboratorios de IA, fundamentalmente gestionados por fondos privados para fines empresariales, están inmersos en una competición desahogada para conseguir mentes digitales cada vez más potentes. Sin embargo, con frecuencia no se ha valorado si los modelos en evolución cumplen estándares adecuados para el tratamiento y monitorización de los datos con los que se alimentan. Tampoco se garantiza la trazabilidad de los criterios utilizados para explicar los resultados, ni que las respuestas estén exentas de sesgos discriminatorios. Esta carencia de control afecta al incremento de las marginaciones y desigualdades sociales.

La IA ofrece enormes oportunidades que tienen que saber aprovecharse para facilitar y mejorar la vida de las personas en diferentes esferas, y la prevención e investigación criminal es una de ellas. Ahora bien, ¿es posible una aplicación ética de la IA que respete los derechos fundamentales en la prevención e investigación del delito?

La reciente entrada de la IA en el ámbito del Sistema de Justicia Penal, en esta cuarta revolución industrial¹, y su vertiginoso desarrollo, ha provocado un vacío científico en este ámbito. Existen partidarios y detractores de la IA, pero esa no es la cuestión, dado que no se puede obviar que el avance y la implementación de la misma es una realidad hoy en día. Por ello, el objetivo principal de la presente investigación consiste en analizar los retos que plantea el uso de esta tecnología en el ámbito del Sistema de Justicia Penal y en concreto en lo que denominamos como IA policial².

Para alcanzar este objetivo principal se han definido los siguientes objetivos específicos: examinar los usos concretos de la IA tanto en la fase preventiva del delito, como en la fase investigativa; comparar los modelos normativos de la Unión Europea (en adelante UE) y de las dos potencias mundiales en esta materia, Estados Unidos y China; identificar los riesgos asociados al uso de la IA en las funciones policiales, con especial atención a la afectación a los derechos fundamentales y las garantías del proceso penal; y proponer criterios éticos para su regulación, integrando reflexiones doctrinales y jurisprudenciales.

Partiendo de los objetivos planteados, la investigación formula la siguiente hipótesis: es posible una aplicación ética de la IA en la prevención e investigación del delito, aunque esta implementación conlleva desafíos regulatorios, técnicos y éticos significativos, por

¹ BARONA (2019), p. 2.

² Véase MIRÓ (2018), p. 97. Establece una clasificación de la IA según si su aplicación se realiza en el ámbito judicial (que denomina IA judicial y que ha centrado la atención de la doctrina) o bien si se utiliza para la prevención e investigación del delito (a la que se refiere como IA policial).

lo que es necesario el diseño de un marco normativo adecuado a la evolución de la tecnología y garantista con los derechos fundamentales y el procedimiento penal.

La investigación se inscribe dentro de un enfoque cualitativo, desarrollado a partir de una lógica deductivo-inductiva. Con el fin de ofrecer un examen integral del fenómeno de la IA en el contexto del Sistema de Justicia Penal y orientado a formular conclusiones regulatorias y éticas, el estudio combina de manera complementaria un análisis dogmático orientado al estudio del ordenamiento jurídico para identificar los principios, valores y derechos fundamentales afectados; un análisis comparativo, para contrastar las principales propuestas normativas y observar las convergencias y divergencias en las tendencias legislativas; y un enfoque analítico-propositivo, a partir del cual se formulan consideraciones éticas y regulatorias encaminadas a promover una aplicación responsable de la IA en el ámbito policial.

Las fuentes empleadas comprenden materiales normativos, jurisprudenciales y doctrinales, seleccionados por su relevancia y actualidad en relación con los objetivos perseguidos.

1. Concepto de IA del que se parte

El uso por primera vez del término IA es atribuido al profesor de la Universidad de Stanford John McCarthy (1927-2011), padre y pionero de esta tecnología, quien en 1955 la definió como “*the science and engineering of making intelligent machines*”. Durante su dilatada carrera como investigador persiguió desarrollar aplicaciones de IA que no se limitaran a imitar el comportamiento humano, sino que tuvieran la capacidad de aprender. Por lo tanto, es necesario subrayar que cuando hablamos de IA no estamos aludiendo únicamente a la capacidad de un gran procesamiento de datos³ o a la automatización de procesos mediante algoritmos⁴ que arrojan unos resultados gracias a la ejecución de las instrucciones con los que han sido codificados, sino que nos referimos a la capacidad autónoma de los sistemas de analizar e interpretar datos mediante el aprendizaje automático⁵ y/o el aprendizaje profundo⁶. Ulteriormente, aparece la IA generativa, la cual es capaz, a partir de este aprendizaje autónomo, de inferir nuevas conclusiones que no habían sido previamente programadas.

De este modo, teniendo en cuenta el grado de interacción entre el humano y la máquina se pueden establecer, siguiendo el modelo de Harbers, Peeters y Neerinx, tres tipos de IA⁷: “*Man in the loop*”, donde la máquina necesita la intervención del humano de manera regular; “*Man on the loop*”, cuando la máquina es capaz de funcionar de manera autónoma pero el humano puede intervenir interrumpiendo o modificando las acciones en cualquier momento; y “*Man out of the loop*”, cuando la máquina funciona de manera

³ Igualmente conocido como *big data*.

⁴ El diccionario de la Real Academia Española define el algoritmo como “Conjunto ordenado y finito de operaciones que permiten hallar la solución de un problema”.

⁵ También llamado *machine learning* definido por la Comunidad Argentina de IA como “el diseño y estudio que utiliza la experiencia pasada para tomar decisiones futuras; es el estudio de programas que pueden aprender de los datos. El objetivo fundamental del *machine learning* es generalizar, o inducir una regla desconocida a partir de ejemplos donde esa regla es aplicada.”, véase GILETTA *et al.* (2020), pp. 24-25.

⁶ También denominado *deep learning* definido por la Comunidad Argentina de IA como “un conjunto particular de algoritmos *machine learning* que utilizan estructuras profundas de redes neuronales para encontrar patrones en los datos”. Véase GILETTA *et al.* (2020), pp. 24-25.

⁷ MIRÓ (2018), *passim*.

independiente y durante algunos periodos de tiempo el humano no tiene influencia en su funcionamiento. Además, otros autores⁸ añaden un cuarto tipo de IA denominada “*No man on the loop*”, para referirse a aquellas decisiones tomadas por la máquina ajenas a la programación humana, es decir, aquellas generadas por el propio sistema.

Este modelo tecnológico de procesamiento masivo de datos, combinado con una capacidad informática enorme y potentes algoritmos, que se está utilizando para predecir, controlar, planear y producir de manera inteligente, no ha quedado restringido a la esfera económica, sino que ha penetrado en todos los ámbitos de la vida. Esto nos ha adentrado en la cuarta revolución industrial⁹ —tras las iniciadas por la introducción del vapor primero, la electricidad después y en tercer lugar los ordenadores—, de la que no ha quedado al margen el Sistema de Justicia Penal.

Muestra de que la IA ha irrumpido en dicho sistema son las aplicaciones de IA surgidas para automatizar determinados procesos jurídicos con los que mejorar la eficiencia y eficacia en el flujo del trabajo judicial. Así, podemos destacar las aplicaciones inteligentes¹⁰ que actúan como asesores jurídicos (*robot lawyers*) para orientar a los ciudadanos en la resolución de problemas legales sencillos; o las herramientas dirigidas a los profesionales del derecho (como son las *startups* de *legaltech*) que mediante la minería de datos¹¹, realizan predicciones de las resoluciones judiciales, incluso teniendo en cuenta el perfil del juez o magistrado juzgador, de manera que ayudan a los abogados a orientar su estrategia de defensa.

Un paso más allá en dicha introducción se encuentran las controvertidas aplicaciones de IA para la determinación judicial de la responsabilidad penal por la perpetración de un delito, o dicho en otras palabras, la sustitución del juez humano por el juez robot¹². Estas herramientas utilizan el *data mining* y el *big data*, de forma que se analiza y procesa gran cantidad de datos, sentencias, jurisprudencia, etcétera, y se elabora una resolución judicial de manera automática. Este tipo de aplicaciones ya se está utilizando en Inglaterra y en Estonia para dictar sentencias en primera instancia en litigios de hasta 10.000 libras esterlinas y 7.000 euros, respectivamente, con la posibilidad de recurso ante jueces humanos¹³.

De hecho, constituye una realidad que la Administración de Justicia se encuentra en pleno proceso de digitalización desde hace unos años¹⁴, lo que ha comportado la realización de sucesivos, aunque lentos, ajustes normativos. La pandemia del COVID-19 supuso un

⁸ (MIRÓ (2018), p. 93; SOUZA DE MENEZES y AGUSTINA (2020), *passim*)

⁹ BARONA (2019), *passim*.

¹⁰ OLIVA (2022), *passim*.

¹¹ La minería de datos o *data mining* es una parte del proceso de extracción de conocimiento a partir de una base de datos (*Knowledge Discovery in Databases*). Esta técnica permite, mediante la aplicación de algoritmos complejos, establecer relaciones ocultas entre los datos y crear patrones, de manera que filtra la información de las bases de datos y predice las salidas. Véase RIQUELME *et al.* (2006), *passim*.

¹² GÓMEZ (2023), *passim*.

¹³ RODRÍGUEZ (2022), p. 3.

¹⁴ Ejemplos de esta digitalización de la Administración de Justicia son, entre otras, las novedades introducidas por el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, tales como los actos procesales mediante presencia telemática (declaraciones por videoconferencia de acusados, testigos y víctimas). Otro ejemplo sería la obtención de las pruebas electrónicas, entendidas como toda aquella información con valor probatorio incluida o transmitida por un medio electrónico.

impulso sin precedentes que hizo aflorar la necesidad de realizar de manera urgente una transformación digital. Este hecho, sumado a una delincuencia transnacional en crecimiento y a un aumento exponencial de la ciberdelincuencia, ha provocado que las diferentes Administraciones realicen un esfuerzo por modernizar el Sistema de Justicia Penal, en el que, como se ha visto, se está introduciendo el recurso a la IA. Constatado esto, en las páginas que siguen se expondrá lo que constituye el objeto principal de este trabajo, la aplicación de la IA en dos ámbitos: el de la prevención policial del delito y el propio de la investigación criminal.

2. Usos de la IA en la prevención delincriminal

La implementación de los sistemas de IA en la prevención policial está ligada a la evolución del actual modelo de policía de proximidad que pretende ofrecer una respuesta proactiva a las demandas de protección de la seguridad ciudadana. De este modo, se persigue establecer una relación de confianza entre los ciudadanos y los cuerpos policiales atacando el delito antes de que se produzca, con la finalidad de aumentar la percepción de seguridad ciudadana y disminuir la criminalidad.

En este contexto, las herramientas de IA generativa para la prevención delincriminal se han introducido como un paso más en el desarrollo tecnológico que se inició con la introducción de técnicas de digitalización en la evitación del delito, como por ejemplo para el control monitorizado de penas¹⁵.

Los sistemas de IA generativa aplicados a la prevención de la criminalidad pretenden ser una herramienta útil para contribuir a mejorar la toma de decisiones por parte de los organismos encargados de hacer cumplir la ley. El objetivo es poder transformar la gran cantidad de información policial en inteligencia y realizar una predicción acertada del delito, para así poder orientar los servicios policiales de prevención de una manera más eficiente y efectiva¹⁶.

Ahora bien, la incorporación de soluciones basadas en la IA en la prevención delincriminal plantea retos éticos y jurídicos, especialmente relacionados con la transparencia, la rendición de cuentas, la explicabilidad de las decisiones automatizadas y la protección de los derechos fundamentales¹⁷.

A continuación se presentan las principales aplicaciones de IA generativa que se están usando en la prevención del delito, señalando sus ventajas y exponiendo sus principales riesgos, en particular: los sistemas para el diseño de mapas criminales, las técnicas de ciberpatrullaje, las aplicaciones para predecir el riesgo de reincidencia delictiva, los

¹⁵ Un ejemplo del uso de este tipo de tecnología serían las pulseras GPS que se usan para controlar la ubicación del penado, ya sea porque tenga prohibido aproximarse a un determinado lugar o a una determinada persona. En España se utiliza este tipo de tecnología en virtud de lo dispuesto en el artículo 64.3 de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, el cual regula entre las medidas para proteger a las víctimas de violencia de género, la prohibición que el inculcado pueda aproximarse a la víctima y prevé que pueda “acordarse la utilización de instrumentos con la tecnología adecuada para verificar de inmediato su incumplimiento”. Este sistema permite que no se deban utilizar medidas más restrictivas para los derechos fundamentales del condenado para evitar su aproximación a la víctima (como sería la permanencia en prisión), además de tratarse de un sistema económicamente más sostenible. Véase OTERO (2008), *passim* y ARENAS (2017), pp. 155-158.

¹⁶ GREENE (2006), *passim*.

¹⁷ GARCÍA (2025), *passim*.

programas para detectar y asesorar a potenciales delincuentes y víctimas, y el software de análisis de la personalidad y predicción delictiva.

2.1. Mapas criminales o *hot spots*

Las aplicaciones de IA destinadas a dibujar los mapas criminales utilizan las técnicas de la minería de datos para procesar la información, hacer aflorar relaciones entre los datos, crear modelos delincuenciales y predecir dónde y cuándo es más probable que suceda un hecho delictivo. Con ello, se pretende dirigir los servicios policiales de manera eficiente para evitar la comisión delictiva, lo que se conoce como policía predictiva¹⁸.

Sin embargo, se plantean algunos inconvenientes, principalmente respecto a la política adoptada para decidir qué tipo de datos alimentan el programa. Veamos un ejemplo, PredPol es un algoritmo utilizado en Estados Unidos para determinar mapas de criminalidad mediante IA. Ahora bien, sus resultados varían sustancialmente dependiendo de si se toman en consideración, por ejemplo, alteraciones leves del orden público, los cuales arrojan resultados de predicción delincuenciales en determinados barrios; o si el sistema se alimenta con los delitos denominados de cuello blanco, los cuales ofrecen resultados muy diferentes, dado que se suelen dar en las zonas financieras de las grandes ciudades¹⁹.

Si a esta diferencia de predicción le sumamos que el patrullaje policial se orientará hacia los barrios donde se producen los desórdenes públicos menores o hacia las zonas financieras (dependiendo de con qué tipo de datos estemos alimentando el programa), es evidente que habrá una mayor detección de nuevos delitos en dichos barrios. En primer lugar, porque al haber más presencia policial se localizarán más desórdenes públicos y, en segundo lugar, por la propia tipología delictiva, resultará improbable que las dotaciones policiales puedan detectar con el patrullaje los delitos económicos. Todo ello provocará que el programa se retroalimente, acentuando la predicción delictiva en los barrios donde se producen los desórdenes públicos menores, sin que se corresponda con un incremento real de la peligrosidad, sino que se deba a la falta de objetividad del mismo programa por los sesgos de los datos de partida.

2.2. Ciberpatrullaje

Cuando nos referimos al ciberpatrullaje estamos aludiendo a aquella actividad de investigación policial que se realiza en el entorno digital, o ciberespacio, antes del conocimiento de que se haya producido un delito y por tanto, de manera previa a la incoación de un proceso penal²⁰.

El medio virtual aparece como un espacio de conectividad universal que se crea con la aparición de Internet y que con el paso del tiempo se ha convertido en un lugar utilizado por millones de personas a diario. Actualmente, según la Unión Internacional de Telecomunicaciones el 67% de la población mundial está conectada en línea²¹. Esto representa que unos 5.400 millones de personas estamos sumidos en el uso de las nuevas tecnologías y las redes sociales. La exposición digital genera una infinidad de datos de

¹⁸ GONZÁLEZ *et al.* (2020), *passim*.

¹⁹ CAMPIONE (2021), p. 134.

²⁰ TAVORA (2023), *passim*.

²¹ Unión Internacional de Telecomunicaciones (2023), *passim*.

nuestras actividades cotidianas²² que proporcionamos, en la mayoría de ocasiones, sin ser conscientes de ello, sin saber quién va a hacer uso de nuestros datos, ni con qué finalidad.

La sobreexposición en el ciberespacio ha creado un nuevo escenario en materia de protección de datos, donde la exhibición en las redes ha reducido la expectativa de privacidad. Los motores de búsqueda rastrean datos digitales, lo que supone, en cierta medida, una injerencia en este derecho fundamental.

Si a esto le sumamos la denominada “guerra contra el terrorismo”²³, iniciada tras los atentados del 11 de septiembre de 2001, junto con la evolución de la “sociedad de riesgo”²⁴ y la consolidación de una corriente que promueve el “derecho penal del enemigo”, se configura un escenario idóneo para que las fuerzas policiales implementen prácticas de vigilancia preventiva basadas en la monitorización de fuentes abiertas²⁵ y redes sociales²⁶. Estas medidas buscan detectar amenazas tanto en el entorno virtual, como fuera de él y se conocen como ciberpatrullaje.

A diferencia de la ciberinvestigación, que persigue delitos ya cometidos y se rige por el marco del proceso penal, el ciberpatrullaje carece de regulación jurídica clara. Esta ausencia normativa puede provocar que la policía realice investigaciones prospectivas que vulneren los principios de especialidad y proporcionalidad. También facilita medidas predelictuales basadas únicamente en la actividad digital de los ciudadanos, clasificándolos como potenciales criminales²⁷.

Todo ello, puede suponer una injerencia injustificada en la intimidad y la protección de datos, incluso de aquéllos que se ofrecen de manera pública, pero sin el conocimiento de su recolección o uso posterior. Asimismo, puede comportar una transgresión de valores fundamentales como la no discriminación y la presunción de inocencia.

La resolución del Parlamento Europeo 2020/2016 sobre IA en el derecho penal y su utilización por las autoridades judiciales y policiales en asuntos penales, de 6 de octubre de 2021, destaca la prohibición de la puntuación de las personas a escala masiva mediante IA y establece la obligación legal de prevenir la utilización de aplicaciones de IA para la vigilancia masiva o para la elaboración masiva de perfiles criminales, ya que no cumplen con los principios de necesidad y proporcionalidad.

Además, advierte de los peligros de los enfoques adoptados por países fuera de la UE (sin mencionarlos se refiere a países como China o Estados Unidos), los cuales han orientado el uso de estas nuevas tecnologías a la vigilancia masiva de sus ciudadanos, lo cual, a criterio del Parlamento Europeo vulnera de manera desproporcionada los derechos fundamentales.

²² Proporcionamos datos desde que nos levantamos usando la alarma del móvil, pasando por los diarios online que leemos, los pagos que efectuamos a través de las aplicaciones en línea, en qué trabajamos, con quién nos comunicamos, cuáles son nuestros intereses y hobbies, cuál es nuestra alimentación, qué viajes hacemos, qué películas o series son de nuestro interés, qué búsquedas on-line realizamos, qué visitas médicas tenemos, cuáles son nuestras tendencias políticas, y un largo etcétera.

²³ HOLLOWAY (2008), p.7.

²⁴ Entendida como una “sociedad catastrófica”, en alerta permanente, constantemente vigilante ante la diversidad de riesgos calamitosos a afrontar. Véase BECK (2019), p. 30.

²⁵ OSINT: *Open-sorce intelligence* o inteligencia de fuentes abiertas.

²⁶ SOCMINT: *Social media intelligence* o inteligencia de medios sociales.

²⁷ MARTÍN (2022), p. 4.

Asimismo, esta resolución prevé el riesgo que comporta el depositar una excesiva confianza en las herramientas de IA atendiendo a la falsa creencia de su rigor científico y objetivo. En este sentido, alerta de la posibilidad que estas aplicaciones repliquen los sesgos discriminatorios de los datos con los que se alimentan, y advierte del peligro de la utilización de algoritmos opacos, entendidos como aquéllos que no utilizan un software de código abierto, y que por tanto no es conocido el modelo matemático utilizado para su toma de decisiones y desarrollo.

Por lo tanto, es necesario abrir un debate para abordar dónde debe el legislador poner los límites entre la necesaria acción de las fuerzas y cuerpos de seguridad para detectar y prevenir el delito en la red, y a la vez preservar el derecho a la presunción de inocencia y a la intimidad de los ciudadanos. El delicado equilibrio entre seguridad y libertad²⁸ debe lograrse después de una reflexión profunda de nuestros principios y analizando el contexto actual de irrupción de las nuevas tecnologías como herramienta, tanto para detectar el delito como para cometerlo. Si bien no se puede poner un cerrojo a la IA, tampoco es aceptable impedir que las autoridades encargadas de hacer cumplir la ley prescindan de unas herramientas que pueden ayudar a detectar conductas en la red que pueden desembocar en graves agresiones para la seguridad, como son los indicadores de polarización en delitos de odio y terrorismo.

2.3. Aplicaciones para la evaluación del riesgo de reincidencia

Los sistemas de IA para la predicción del riesgo de reincidencia delictiva se basan en el uso de datos históricos para generar patrones y evaluar la probabilidad que un individuo vuelva a delinquir, con el objetivo de ayudar al juzgador a la toma de decisiones y limitar la arbitrariedad judicial²⁹. Estas aplicaciones han sido profundamente criticadas tanto por establecer patrones estadísticos que no se corresponden con las circunstancias en las que se ha cometido el delito, sino con la peligrosidad que supone el (todavía) presunto autor para la sociedad, lo que conlleva discriminaciones contra determinados grupos sociales; así como por la opacidad de sus algoritmos, lo que implica una vulneración del derecho a contradicción por parte de los evaluados, al ser imposible rebatir el resultado del programa sin conocer su diseño³⁰.

Un ejemplo es el sistema COMPAS³¹ utilizado en Estados Unidos para evaluar el riesgo de reincidencia de los delincuentes. Este programa está diseñado para clasificar con la misma puntuación predictiva a personas diferentes con características similares. El programa establece patrones predictivos de los acusados no condenados a partir de: los antecedentes, las detenciones previas, la delincuencia en su vecindario, el consumo de drogas de sus amigos, sus notas en la escuela, el número de detenciones de su figura

²⁸ FERNÁNDEZ (2019), *passim*.

²⁹ PLANCHADELL (2021), *passim*.

³⁰ En materia de transparencia algorítmica, el Tribunal Supremo de España, en su sentencia núm. 1119/2025, de 11 de septiembre, se pronunció por primera vez sobre el acceso al código fuente de una aplicación pública. En dicho fallo, el Tribunal reconoció el derecho de la Fundación Ciudadana Civio a acceder al código fuente del programa informático BOSCO, empleado para determinar la elegibilidad de los solicitantes del bono social eléctrico. Esta resolución constituye un precedente relevante en proteger la transparencia y la rendición de cuentas de los sistemas automatizados utilizados en la gestión de derechos sociales, al subrayar que la opacidad algorítmica puede afectar a la protección de derechos fundamentales vinculados a la justicia, la equidad y la igualdad en la asignación de recursos públicos.

³¹ *Correctional Offender Management Profiling for Alternative Sanctions*.

paterna, si alguna vez ha oído o visto cosas a su alrededor que no eran reales, entre otras. De esta manera, la aplicación arroja una puntuación que va de 1 a 10, donde 1 se corresponde a un nivel de predicción bajo de reincidencia, mientras 10 es el nivel más alto. La guía de usuario de COMPAS muestra los tipos y las principales escalas de evaluación (reincidencia general, reincidencia violenta y mala conducta previa al juicio), pero no determina qué criterios utiliza el algoritmo, ni cómo influye cada escala en el resultado obtenido³².

Parece obvio que algunas de las preguntas utilizadas por el programa pueden vulnerar la presunción de inocencia, afectar a la intimidad del examinado, utilizar datos de su salud mental para mantenerlo o ingresarlo en prisión y no para proporcionarle un tratamiento médico, así como contener desviaciones en su nivel predictivo atendiendo a prejuicios clasistas o raciales. En este sentido destaca la investigación que ProPublica³³ realizó del programa COMPAS, en la cual se realizó un seguimiento de 7.200 personas evaluadas por el programa para determinar si el nivel de riesgo otorgado por la aplicación se correspondía o no con la realidad, y si factores como la raza de las personas examinadas afectaban en el resultado, tanto de los falsos positivos³⁴ como de los falsos negativos³⁵. La investigación evidenció³⁶ que COMPAS ofrece resultados con un evidente sesgo racial, ya que respecto a los falsos positivos, el 11% de los blancos encarcelados no volvieron a ser detenidos, frente al 32% de negros. Y por lo que respecta a los falsos negativos, el 65% de blancos liberados fueron nuevamente detenidos, frente al 32% de negros.

Asimismo, COMPAS ha sido insistentemente cuestionado y criticado por la opacidad de sus algoritmos, ya que la empresa que lo desarrolló (Northponte) se niega a dar a conocer su diseño, alegando derechos a la propiedad intelectual. Esto provoca que los evaluados no puedan ejercer el derecho a contradecir sus resultados, debido a que no conocen el diseño de la toma de decisiones que aboca en la puntuación del nivel de riesgo que se les asigna³⁷.

Igual de opaca ha sido la aplicación SyRI³⁸ utilizada en Países Bajos para predecir el riesgo de defraudar al Estado. En este caso, el algoritmo no quiso hacerse público por parte del gobierno no porque perteneciera a una empresa privada, sino para evitar que los ciudadanos, a los que se trató como potenciales delincuentes, tuvieran el conocimiento suficiente para desarrollar las herramientas necesarias para poder engañar al algoritmo.

³² ROA *et al.* (2022), *passim*.

³³ ANGWIN *et al.* (2020), *passim*.

³⁴ Personas que habían sido calificadas con un alto riesgo de reincidencia, pero que no habían vuelto a ser detenidas.

³⁵ Personas que pese a haber obtenido un riesgo bajo de reincidencia sí habían vuelto a ser detenidas.

³⁶ HAO (2021), *passim*.

³⁷ Eric Loomis fue condenado por la Corte Suprema de Wisconsin y en su sentencia se le apreciaba alta probabilidad de reincidencia a tenor de los resultados obtenidos por el programa COMPAS. Loomis solicitó acceso al software del programa para poder refutarlo, pero le fue denegado alegando que el programa estaba cubierto por la propiedad intelectual de la empresa privada a la que pertenecía. En la revisión de la cuantía de la pena que solicitó Loomis al tribunal, entre otras razones, exponía que se había vulnerado su derecho a un proceso debido al fundamentarse la sentencia en el resultado arrojado por el programa COMPAS para la evaluación de su riesgo de reincidencia delictiva. El tribunal no modificó la condena y expuso que sólo había utilizado el programa para corroborar las conclusiones a las que ya había llegado por otras vías. Véase la sentencia de la Corte Suprema de Wisconsin (Estados Unidos): *State v. Loomis*, 881 N.W.2d 749, de 13 de julio de 2016.

³⁸ *System Risk Indication*.

A este respecto, el Tribunal de Distrito de la Haya³⁹ consideró que SyRI vulneraba el derecho a la privacidad recogido en el artículo 8 del Convenio Europeo de Derechos Humanos, dado que utilizaba los datos económicos de los contribuyentes (los cuales no carecían de sesgos discriminatorios) para predecir el riesgo que tenían de defraudar al Estado, concluyendo que el interés público para la prevención del fraude no justificaba la vulneración a la privacidad de los ciudadanos.

Otro ejemplo de aplicación de IA para evaluar el riesgo de reincidencia, de fiabilidad dudosa, es VioGen⁴⁰. Dicho sistema se está utilizando en España desde 2007 para medir el riesgo que las víctimas de violencia de género o sus hijos puedan volver a sufrir una agresión, y realizar así una valoración de qué nivel de seguimiento y protección se les debe realizar⁴¹.

El sistema VioGen se inicia con un cuestionario de valoración policial de riesgo⁴², cumplimentado en sede policial cuando una víctima de violencia de género presenta la denuncia. El sistema responde otorgando uno de los cinco niveles de riesgo (no apreciado, bajo, medio, alto y extremo) y en función del resultado se adoptan las medidas de protección que se consideran más adecuadas⁴³. Posteriormente, la policía realiza un seguimiento de la víctima y hace un segundo cuestionario de valoración policial de la evolución del riesgo. Estas valoraciones de riesgo son diligenciadas por el instructor del atestado para informar al órgano judicial competente, así como al Ministerio Fiscal. De este modo se pretende ofrecer una herramienta que está en continuo proceso de mejora y que obvia la subjetividad del evaluador. Ahora bien, la complejidad de los formularios, su artificialidad y una inadecuada parametrización pueden provocar que no se adopten unas medidas de protección congruentes con el caso en cuestión.

Pese a que el sistema prevé que el nivel de riesgo asignado pueda ser modificado al alza por el policía instructor de las diligencias, de manera que no recaiga la responsabilidad de las medidas de protección en un algoritmo⁴⁴, lo cierto es que es habitual que la policía caiga en el automatismo de confirmar la puntuación obtenida de VioGen, y que a su vez esto arrastre a las autoridades judiciales en el mismo sentido⁴⁵.

La sentencia de la Audiencia Nacional número 2350/2020, de 30 de septiembre, se pronuncia al respecto⁴⁶ del recurso contencioso-administrativo contra la resolución de desestimación de la responsabilidad civil por parte del Estado, en el caso de la muerte de una víctima de violencia de género a manos de su esposo, la cual había solicitado una orden de protección después de denunciarse mutuamente por agresiones. Los agentes de

³⁹ Corte de Distrito de La Haya. ECLI:NL:RBDHA:2020:1878, de 5 de febrero de 2020.

⁴⁰ Sistema de Seguimiento Integral en los casos de violencia de género.

⁴¹ Esta aplicación fue creada para dar cumplimiento al artículo 32 de la Ley 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género, según la Orden INT/1911/2007, de 26 de junio, la cual se actualizó por la Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior.

⁴² GONZÁLEZ *et al.* (2018), pp. 209-212.

⁴³ En atención a lo previsto en la Instrucción 7/2016, de 8 de julio, de la Secretaría de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (Ley Orgánica 1/2004) y de gestión de la seguridad de las víctimas.

⁴⁴ MONTESINOS (2021), *passim*.

⁴⁵ ESTÉVEZ (2020), p. 136.

⁴⁶ ESTÉVEZ (2020), p. 129-131.

policía hicieron una valoración del riesgo que fue calificada como “no apreciado”, por lo que le fue denegada la orden de protección por el Juzgado de Primera Instancia e Instrucción en la celebración del juicio rápido, aludiendo entre otras razones a la calificación del riesgo realizada, y finalmente la mujer fue asesinada por su marido.

El fallo señala que no se tuvieron en cuenta (ni por parte de la policía, ni por parte de la jueza de instrucción, a quién le compete de manera exclusiva acordar o no la orden de protección) condicionantes particulares de la víctima como los antecedentes del agresor en su país de origen, denuncias previas por parte de la denunciante contra su marido, entre otras, por haber sido obligada a mantener relaciones sexuales con él, aunque habían sido posteriormente no ratificadas. Por esto la resolución condena al Estado a indemnizar a los familiares de la víctima por haber realizado una incorrecta valoración del riesgo, dado que no se indagó en apreciar las circunstancias concretas de la víctima a la hora de realizar la valoración de riesgo.

A lo expuesto, cabe añadir, para cuestionar la fiabilidad de VioGen, el aumento en los últimos años de los feminicidios y de los menores de edad víctimas mortales en casos de violencia de género contra su madre en España, pese a la insistencia de las autoridades gubernamentales de reforzar e invertir en este sistema para contrarrestarlos⁴⁷.

2.4. Asesoramiento a potenciales delincuentes y víctimas para evitar el delito

La IA también se está utilizando para el asesoramiento a potenciales delincuentes y posibles víctimas para evitar que lo sean. Por ejemplo, en Inglaterra, se utiliza el algoritmo NDAS⁴⁸ que, a partir de 1.400 indicadores de delitos cometidos y personas detenidas, predice la comisión de un crimen violento, el nivel de riesgo de que un individuo cometa un delito con arma blanca o de fuego y el riesgo de quién puede ser víctima⁴⁹. Teniendo en cuenta estas predicciones se activan los recursos de servicios sociales adecuados para alertar, atender, advertir y asesorar tanto a potenciales victimarios, como posibles víctimas, antes de que suceda el hecho delictivo para intentar evitarlo.

Este tipo de algoritmos pueden ayudar a ofrecer a las potenciales víctimas información y protección, sobre todo en materia de trata de seres humanos⁵⁰ o en las solicitudes sexuales online a menores, para que sean capaces de identificarse como víctimas de un delito e informarles de los recursos y la protección policial de la que pueden disponer. Por su parte, a los posibles victimarios se les muestran las conductas que son susceptibles de ser

⁴⁷ Según publica el Ministerio de Igualdad las mujeres víctimas mortales por violencia de género en España a manos de sus parejas o exparejas en 2021 fueron 49, en 2022 fueron otras 49, en 2023 ascendieron a 58 y en 2024 (hasta el 16 de julio) han sido 27. Por su parte, los menores víctimas mortales por violencia vicaria en 2021 fueron 7, en 2022 fueron 2, en 2023 otros 2 y en los que va de 2024 (hasta el 16 de julio) han ascendido hasta 9. Véase <https://violenciagenero.igualdad.gob.es/violenciaencifras/victimasmortales/fichamujeres/> y <https://violenciagenero.igualdad.gob.es/violenciaEncifras/victimasMortales/fichaMenores/>

⁴⁸ *National Data Analytics Solution*.

⁴⁹ ROA *et al.* (2022), p. 281.

⁵⁰ Las nuevas tecnologías están siendo utilizadas como instrumento eficaz de captación, explotación, chantaje y control, de víctimas de trata de seres humanos por los *lover boys*, beneficiándose del anonimato que las redes sociales ofrecen. Ahora bien, las ventajas del uso de estas herramientas también deben de ser aprovechadas por las autoridades encargadas de hacer cumplir la ley para detectar estas conductas y evitarlas. Véase PLANCHADELL (2023), pp. 400-401.

penadas y sus consecuencias, se les ofrecen servicios sociales, de salud u otros, con el objetivo que desistan antes de delinquir.

Si bien estas herramientas pueden resultar útiles para evitar el delito antes de que se cometa, pueden conllevar significativas injerencias en derechos como la presunción de inocencia de los señalados como potenciales futuros delincuentes. Además, no cabe menospreciar los cambios de conducta en su vida cotidiana que pueden acarrear para las apuntadas como posibles víctimas con base en “indemostrados pánicos morales”⁵¹, con su consecuente afectación, entre otros, al derecho a la libertad no solo de movimiento en el mundo físico, sino también en el virtual, por miedo a ver cumplida la predicción a la que se les ha sometido.

2.5. Aplicaciones de análisis de la personalidad y predicción delictiva

Acontecimientos como los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos marcaron un punto de inflexión en las políticas de seguridad de los países occidentales que se ha ido extendiendo al resto del mundo. Se ha optado por inclinar el siempre delicado equilibrio entre seguridad y derechos humanos hacia la protección de la seguridad. Y lo han hecho adoptando un enfoque contrapuesto⁵² entre seguridad y derechos humanos, en sentido negativo, como si solo fuera posible más seguridad a costa de menguar la libertad o la privacidad; y no poniendo el foco en el sentido positivo de esta yuxtaposición, cuando indudablemente, delante de una sociedad más segura vamos a poder ejercer nuestros derechos fundamentales de una manera más amplia y profunda.

En este contexto, el uso de la IA como herramienta para analizar conductas de la personalidad y predecir un comportamiento delictivo está creciendo en multitud de países. Un ejemplo es China, que está utilizando un sistema de IA creado en 2015 y llamado Cloud Walk, que pretende prevenir el crimen antes de que ocurra haciendo una predicción del comportamiento humano. Para ello se basan en el reconocimiento facial, el análisis de la marcha y de los demás datos que tienen monitorizados de sus ciudadanos para predecir cuáles son más propensos a cometer un delito⁵³.

De esta manera, la policía china está realizando una clasificación de sus ciudadanos, señalando grupos de personas de alto riesgo delictivo, en función de dónde van y qué hacen. El sistema tiene memoria, así es capaz de reconocer a la misma persona, aunque lleve ropa diferente, monitoriza qué tiendas visita, qué compra, dónde va, y hace una relación de estos parámetros para predecir si se puede tratar de un potencial delincuente. El programa incluso detecta comportamientos anormales de personas en medio de grandes multitudes (tipo carteristas) y alerta a las autoridades. El problema que se plantea es que, una vez que el sistema ha apuntado a un individuo como persona de alto riesgo delictivo, dicho sujeto tiene escasa posibilidad de recurrir y contradecir el resultado arrojado por esta IA.

⁵¹ VILLACAMPA y GÓMEZ (2016), p. 23.

⁵² FERNÁNDEZ (2019), *passim*.

⁵³ HERNÁNDEZ (2019), p. 831.

Por su parte, Estados Unidos dispone del sistema FAST⁵⁴, que se utiliza para analizar los datos de los pasajeros de los aviones (frecuencia cardíaca, mirada, etcétera) para predecir la probabilidad que vayan a cometer un delito relacionado con el terrorismo⁵⁵.

La UE entre 2016 y 2019 financió el desarrollo del proyecto IBorderCtrl⁵⁶ que usa tecnología de IA con el objetivo de facilitar, agilizar y mejorar el control de los procesos del cruce de fronteras. Este sistema introduce el registro previo a la llegada de los viajeros a la frontera, realiza una evaluación de los riesgos y de los intentos de engaño a los agentes fronterizos por parte de los transeúntes, utiliza tecnología biométrica para verificar la identidad y detectar emociones, hace una predicción del movimiento de los viajeros en los pasos fronterizos, así como establece patrones predictivos a partir de los datos históricos⁵⁷. Esta herramienta ha sido objeto de controversia, dado que se ha puesto en duda su validación científica, tanto por el insuficiente tamaño de la muestra del conjunto de datos utilizados para el entrenamiento de los algoritmos, como por la inexistencia de resultados que avalen que el sistema alcanza el rendimiento propuesto en su diseño⁵⁸.

Asimismo, se están utilizando técnicas de análisis de reconocimiento facial y corporal para detectar microexpresiones y gestos que denoten señales de intranquilidad o nerviosismo, que puedan alertar de la determinación de que un sujeto tiene la voluntad de delinquir. Un ejemplo de este tipo de software es Vaak⁵⁹ utilizado en las tiendas de Japón para prevenir que se cometan hurtos o robos. Las imágenes captadas por las cámaras de seguridad de los locales son analizadas mediante esta aplicación y alertan a los dependientes del comportamiento anómalo de algún cliente, para que puedan prestarle atención, requerirle si necesita ayuda y disuadirlo de esta manera de cometer la sustracción antes de que se produzca.

También en este ámbito, la policía de Chicago utiliza un sistema de IA para predecir qué ciudadanos son más propensos a disparar un arma y a ser disparados (basándose en las veces que una persona ha sido arrestada, las veces que ha efectuado disparos o si pertenece a una banda callejera)⁶⁰ y así orientan sus servicios policiales a hacer una supervisión presencial de ellos. Si bien la herramienta está pensada para evitar los altercados con arma de fuego, no está exenta de polémica. Por un lado, porque puede vulnerar el derecho a la presunción de inocencia de los señalados como personas de alto riesgo a usar un arma de fuego al estar sobre vigilados por la policía; y, por otro lado, porque para los marcados con un alto riesgo de ser disparados puede conllevar una alteración de su vida cotidiana debido a la ansiedad a recibir un disparo que merme su libertad deambulatoria.

3. Usos de la IA en la investigación criminal

Si en las precedentes páginas se ha hecho referencia a los instrumentos a través de los cuales se ha introducido la IA en la prevención policial del delito, destacando sus ventajas y sus inconvenientes, en las que siguen se hará lo propio con el recurso a la IA generativa

⁵⁴ *Future Attribute Screening Technology*.

⁵⁵ UNITED STATES DEPARTMENT OF HOMELAND SECURITY (2014), *passim*.

⁵⁶ *Intelligent Portable Border Control System*.

⁵⁷ COMISIÓN EUROPEA (2021), *passim*.

⁵⁸ SÁNCHEZ y DENCİK (2020), *passim*.

⁵⁹ VAAK (2023), *passim*.

⁶⁰ HERNÁNDEZ (2019), p. 832.

en el segundo de los ámbitos analizados, el de la investigación criminal. Tradicionalmente el investigador criminal se ha caracterizado por recopilar gran cantidad de datos de las escenas de los crímenes, de los testigos y de las circunstancias que rodean al hecho delictivo con el objetivo de analizarlos, descartar los datos inservibles, hacer aflorar los relevantes y ser capaz de relacionarlos. Todo ello con la finalidad de averiguar qué ha ocurrido, cuándo, dónde, quién ha sido el autor o autores y cuál es el móvil. El propósito es poder establecer un *modus operandi* para poderlo cotejar y comparar con otros casos e intentar examinar similitudes y coincidencias que ayuden a esclarecer los crímenes.

Este proceso requiere la utilización de un método riguroso y una alta formación por parte del investigador a la hora de recoger los datos que deberá procesar. También será necesaria una dilatada trayectoria profesional que le ayude a realizar un análisis acertado de toda la información de la que dispone, a fijarse en los detalles importantes y descartar los que no lo son. Además, este proceso requiere tiempo para poder explotar las bases de datos de manera eficiente, transformar la información de la que dispone en inteligencia, así como para explorar las diferentes líneas de investigación hasta dar con la acertada y ser capaz de realizar una comparativa adecuada con otros casos para obtener pruebas para resolverlos.

Un uso adecuado de la IA en la investigación criminal puede reducir este complejo y elaborado proceso a un simple *click* en una aplicación; pero las ventajas no son únicamente cuantitativas (respecto al tiempo empleado), sino que también son cualitativas, como se señala a continuación.

3.1. Procesamiento y análisis de la escena del crimen

La IA puede convertirse en una herramienta esencial para los investigadores a la hora de procesar y analizar la escena de un crimen, filtrar y comparar los datos obtenidos de manera automática con las diferentes bases de datos, procesar documentos, leer matrículas, analizar imágenes, huellas, fluidos, ADN, identificar o verificar la identidad de una persona mediante análisis de datos biométricos (ya sea víctima, testigo o sospechoso). También para realizar y analizar las declaraciones necesarias para acreditar las circunstancias en las que se ha cometido el hecho delictivo. Todo ello con la finalidad de averiguar quién ha sido su autor, optimizando los recursos humanos, materiales y el tiempo empleado.

Un ejemplo de esta tecnología lo constituye el proyecto VALCRI⁶¹, iniciado en 2018 por el profesor Willian Wong y financiado por la UE, que está siendo desarrollado en países como Reino Unido y Bélgica de manera experimental. Este sistema consta de más de 75 herramientas de IA basadas en análisis visuales e ingeniería cognitiva⁶².

El programa procesa la escena de un crimen mediante los datos obtenidos por los investigadores, fotografías, vídeos, declaraciones de víctimas, testigos, sospechosos, etcétera. A partir de esta información, la aplicación recrea diferentes reconstrucciones de manera visual, relacionando los datos y exponiendo diferentes explicaciones para facilitar la comprensión y el trabajo de los investigadores. Para ello, VALCRI utiliza la ingeniería cognitiva basada, en primer lugar, en la observación de los datos y cómo se relacionan

⁶¹ *Visual Analytics for Sense-making in CRiminal Intelligence analysis.*

⁶² COMISIÓN EUROPEA (2023), *passim*.

entre sí; en segundo lugar, en el análisis de patrones, tendencias y comportamientos relevantes; y, en tercer lugar, elabora hipótesis para ofrecer razonamientos científicamente comprobables que muestran las líneas de investigación más plausibles a los investigadores.

El sistema ofrece una manera manejable de relacionar la gran cantidad de datos obtenidos, permite que afloren detalles que podrían ser pasados por alto por los analistas o cuya valoración les requeriría gran cantidad de tiempo, facilita la relación y comprensión de conceptos y genera razonamiento mostrando propuestas de lo que puede haber sucedido. VALCRI utiliza herramientas de reconocimiento facial que coteja mediante IA con los datos contenidos en el *big data* en tiempo real, de manera que en breves instantes de tiempo es capaz de identificar un sospechoso, una víctima o una persona de interés para la investigación⁶³.

Al ser capaz de organizar y relacionar gran cantidad de datos, VALCRI también permite realizar búsquedas avanzadas de manera rápida. El sistema extrae una gran cantidad de datos de los informes de delitos en función de listas de palabras según su semántica. Así, realiza múltiples clasificaciones, por ejemplo, respecto a conceptos como materiales, de manera que el programa es capaz de clasificar los casos de robos sufridos en viviendas en los que la puerta era de madera, de acero, u otro material; o bien es capaz de clasificarlos en función de si la puerta estaba abierta o cerrada.

Además, VALCRI como sistema de IA que es, aprende y evoluciona con su uso, por lo que cada vez presenta mejores resultados. De esta manera, el sistema está diseñado para desarrollar conocimiento y brindarlo a los analistas e investigadores para facilitarles su labor. El proyecto está pensado para ofrecer un enfoque imaginativo, riguroso, coherente, manejable y científicamente comprobable que promueve el trabajo conjunto entre la IA y los humanos.

Los desarrolladores de este prototipo, todavía en fase de evolución, están trabajando en garantizar que el funcionamiento de VALCRI sea respetuoso con las leyes de protección de datos de la UE. Por este motivo, se están preocupando en lograr una efectiva anonimización de los datos con los que alimentan al sistema, incluso la de aquellos que resulta más dificultosa porque deben de seguir manteniendo las relaciones entre entidades sin que sea posible revertir su anonimato⁶⁴.

3.2. Reconocimiento de patrones biométricos

El reconocimiento de patrones biométricos es utilizado desde hace años para identificar⁶⁵ y/o verificar⁶⁶ la identidad de una persona. Los mecanismos más comunes son el

⁶³ PASTORINI (2020), *passim*.

⁶⁴ COMISIÓN EUROPEA (2023), *passim*.

⁶⁵ Mediante un tratamiento técnico se crea una plantilla de los datos biométricos de la persona a identificar y esta plantilla se compara con otras plantillas de datos biométricos almacenadas en una base de datos. De manera que se realiza un cotejo de correspondencias “uno-a-varios”. Véase el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE.

⁶⁶ En esta ocasión, la plantilla de datos biométricos del candidato se compara únicamente con una plantilla para corroborar su coincidencia, de forma que la comparativa se realiza “uno-a-uno”. Véase el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE.

reconocimiento dactilar, facial, del iris, de la voz y de ADN. Se trata de cotejar uno o más datos inalterables pertenecientes a un individuo con los de una base de datos para determinar su identidad.

El Parlamento Europeo y el Consejo de la UE han definido⁶⁷ los datos biométricos como “datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”. Por lo tanto, los datos biométricos están considerados dentro de la categoría de “datos personales” y además, el artículo 9 del Reglamento 2016/679 les dota de una especial protección, debido a la “intensa injerencia en la privacidad del interesado”⁶⁸, ya que “revelan información muy sensible, no sólo porque se trata de datos personales, sino también porque son permanentes”⁶⁹.

Además se deberá tener en cuenta que, en el contexto de la UE, la utilización de datos biométricos en el entorno policial estará sujeta a lo establecido en el artículo 10 de la Directiva (UE) 2016/680, que restringe su uso a la estricta necesidad y siempre salvaguardando los derechos y libertades del interesado.

Actualmente, Interpol⁷⁰ es un ejemplo de buenas praxis en compartición policial de información biométrica mediante el Sistema Mundial de Comunicación Policial I-24/7⁷¹ (Información 24 horas, 7 días a la semana). Este sistema consta de 19 bases de datos⁷²

⁶⁷ Artículo 4.14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Artículo 3.18 del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

Artículo 3.13 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

⁶⁸ FREIRE (2022), p.68.

⁶⁹ GARTLAND (2016), p.1.

⁷⁰ Interpol (Organización Internacional de Policía Criminal) es una organización intergubernamental que cuenta con 195 países miembros que coordina y facilita el intercambio de información a las policías de los diferentes países miembros, con la finalidad de combatir el crimen.

En cada país miembro hay una Oficina Central Nacional que actúa como enlace y punto de contacto con la Secretaría General de la organización, por lo que Interpol no dispone de policías propios, sino que está formada por la coordinación y el intercambio de información de las diferentes policías de los estados miembro.

⁷¹ INTERPOL (2024), *passim*.

⁷² Bases de datos de Interpol:

- Individuos: datos personales y antecedentes; base de datos internacional sobre explotación sexual de niños (comparación de imágenes para establecer conexiones entre víctimas, agresores y lugares)
- Investigación forense: huellas dactilares, ADN, I-familia (personas desaparecidas o búsqueda de familiares mediante cotejo ADN), reconocimiento facial.
- Documentos oficiales y de viaje: documentos identidad y de viaje, documentos administrativos robados, documentos falsos, comparación documentos auténticos y falsos.
- Bienes robados: vehículos de motor, embarcaciones, obras de arte.
- Tráfico de armas de fuego: identificación, rastreo, comparación de datos balísticos.

que contiene información sobre delincuentes y delitos, que ofrecen un tiempo medio de respuesta desde cualquier parte del mundo de 0,5 segundos y que en 2021 proporcionó 1,3 millones de coincidencias positivas, las cuales sin duda contribuyen al avance de las investigaciones. Interpol dispone de un marco jurídico⁷³ sólido que ofrece cobertura legal al intercambio de información entre los países miembros para garantizar la eficacia y la calidad de sus resultados.

El reconocimiento facial en la investigación criminal se utiliza habitualmente para determinar o verificar la identidad de un sujeto cuya actuación delictiva ha quedado previamente registrada, ya sea por cámaras de grabación instaladas para la prevención del delito, o por imágenes obtenidas por los investigadores policiales en su cometido de averiguación e investigación criminal. De esta manera se obtienen imágenes dubitadas del autor de un ilícito penal (del que se desconoce su identidad) que son comparadas con imágenes indubitadas (de las que se conoce irrefutablemente su identidad) correspondientes a los posibles candidatos, las cuales se encuentran en las bases de datos policiales, como imágenes de las reseñas policiales o de los documentos de identidad. El análisis de los rasgos faciales mediante técnicas precisas y científicas es realizado por especialistas que actuarán como peritos en el procedimiento penal para dar cuenta de su trabajo y someterlo a contradicción en el juicio oral.

Esta técnica goza del respaldo normativo necesario en España para poder ser realizada por la policía en su labor de investigación y tener validez como prueba en el procedimiento penal cumpliendo con las garantías procesales necesarias, pese a que no esté expresamente regulada en la Ley de Enjuiciamiento Criminal. Esta cobertura normativa la encontramos en el artículo 13.2 de la LO 7/2021⁷⁴, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el cual establece que “Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública”.

Ahora bien, actualmente está abierto el debate respecto a la utilización del reconocimiento facial automático, entendido como el uso de técnicas de IA para comparar de forma masiva imágenes captadas por cámaras de videovigilancia en puntos de interés, con imágenes de individuos almacenadas en las bases de datos.

En este ámbito cabría destacar dos enfoques del uso del reconocimiento facial masivo, uno que estaría íntimamente ligado con la prevención delincriminal, cuando es usado antes de que suceda un hecho delictivo, como herramienta de control y evitación. Y un segundo enfoque, que estaría relacionado con la hipervigilancia en la investigación

-Redes de delincuencia organizada: piratería marítima.

⁷³ Este marco jurídico de Interpol se integra por: el Estatuto de 1956, el Reglamento General, el Reglamento Interno de la Asamblea General y el Comité Ejecutivo, el Reglamento Financiero, el Reglamento sobre el Tratamiento de Datos y el Estatuto de la Comisión de Control de los Ficheros de Interpol.

⁷⁴ El legislador español ha transpuesto mediante el artículo 13 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el artículo 10 de la Directiva (UE) 2016/680.

criminal, usando este tipo de tecnología para el reconocimiento e identificación masivo de delincuentes buscados, cotejando las imágenes obtenidas por las cámaras de videovigilancia en lugares públicos, aeropuertos u otros puntos de interés, con las imágenes de los criminales buscados. En ambos casos, cabría debatir nuevamente entre la colisión de los derechos fundamentales y el derecho a la seguridad pública, y ponderar adecuadamente en base al principio de proporcionalidad dónde situar los límites.

El uso del reconocimiento facial para la investigación criminal es una realidad hoy en día por parte de diferentes agencias, policías y organismos internacionales. Tal y como se ha señalado anteriormente, Interpol está haciendo uso desde 2016 de esta técnica. En Estados Unidos una cuarta parte de los cuerpos policiales también usan este tipo de tecnología⁷⁵.

En China se utiliza el cotejo de las imágenes obtenidas por cámaras de videovigilancia en lugares públicos, conciertos, centros comerciales, u otros lugares de interés, con las imágenes de delincuentes buscados, así como por las imágenes obtenidas de gafas de reconocimiento facial que portan los agentes de policía, técnicas que han comportado la detención de múltiples delincuentes. Estas aplicaciones forman parte del actual programa de control social chino. En este país se ha diseñado un sistema gubernamental de vigilancia extensiva de toda la población. Con esta finalidad, se han instalado más de 500 millones de cámaras⁷⁶ con tecnología de IA para detectar infracciones de todo tipo e identificar a sus responsables. Asimismo, se ha implementado un sistema de “crédito social”, según el cual las personas que se clasifican como “personas no confiables” tienen limitados sus derechos, no pudiendo acceder a cierto tipo de servicios, trabajos, formación, educación, sanidad, créditos, transporte público, vivienda, deducciones fiscales, etcétera.

El hecho que esta hipervigilancia se esté llevando a cabo en China, no supone que en los países democráticos occidentales se vaya a aceptar su implementación sin controversia. De hecho, el Georgetown Center on Privacy and Technology⁷⁷ alerta de que el debate que se suele generar en torno a la privacidad en el uso de este tipo de tecnología no pone de relieve los sesgos de raza, clase social, nivel económico o poder. Y destaca que los algoritmos de reconocimiento facial ofrecen diferentes problemas como son, en síntesis, la imposibilidad por parte de los acusados mediante esta técnica de impugnar su imputación. También señala que el uso inadecuado del reconocimiento facial ha provocado detenciones sin tener en cuenta otros elementos que ofrecían indicios de lo contrario, con las graves consecuencias que esto conlleva para los afectados, así como para la perpetuidad de los sesgos discriminatorios.

Clearview IA es una aplicación de reconocimiento facial mediante el uso de IA que va un paso más lejos. En este caso, el programa coteja las imágenes de los individuos a identificar (sospechosos, testigos y/o víctimas) con millones de imágenes que circulan en

⁷⁵ GARVIE *et al.* (2016), *passim*.

⁷⁶ Según publicó *The Wall Street Journal*, IHS Market calculó en 2019 que había 1.000 millones de cámaras de vigilancia en el mundo, de las cuales un 54% (unos 540 millones) estaban ubicadas en China, país que cuenta con una población de 1.460 millones de habitantes, aproximadamente, lo que comporta que hay 372,8 cámaras por cada 1.000 personas. Véase LIN y PURNELL (2019), *passim*.

⁷⁷ Grupo de expertos de la Universidad de Georgetown, en Washington DC, que estudia el impacto del uso de la tecnología en el rastreo del cuerpo humano, la afectación a la privacidad, los sesgos discriminatorios de los datos y los algoritmos, y la falta de una legislación adaptada al siglo XXI que ofrezca una cobertura legal adecuada a la presunción de inocencia de los sospechosos inculcados por la tecnología de vigilancia.

Internet, incluidas las redes sociales. Este software creado en 2017 en Estados Unidos ha generado múltiples alertas por la posible vulneración a la intimidad y a la protección de datos personales, ya que la recolección de imágenes de forma masiva en la red no se ha efectuado con el debido consentimiento (y en numerosas ocasiones con el desconocimiento) de las personas afectadas.

Por este motivo, el uso de Clearview IA ha sido sancionado⁷⁸ en diferentes países de la UE, tales como Italia, Francia y Grecia, por incumplir los principios fundamentales del Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Se considera que infringe los principios relativos al tratamiento de los datos y su licitud (artículo 5 y 6), el tratamiento de categorías especiales de datos personales donde quedan incluidos los “datos biométricos dirigidos a identificar de manera unívoca a una persona física” (artículo 9), la información que deberá facilitarse cuando los datos personales se obtengan del titular de los datos (artículo 13), así como cuando no se obtengan del interesado (artículo 14) y los derechos de acceso de la persona afectada (artículo 15).

La UE está mostrando una especial sensibilidad respecto a la preservación de los derechos fundamentales de la privacidad y de la protección de datos personales en el uso de las tecnologías de reconocimiento facial⁷⁹. Esta preocupación queda patente en el Informe de la Agencia Europea de Derechos Fundamentales (FRA) de 2019, que alude a la necesaria preservación de un elevado nivel de protección de los derechos fundamentales en el uso de las nuevas tecnologías, y establece que los Estados miembros “deberían situar los derechos fundamentales en el centro de las estrategias nacionales en materia de inteligencia artificial y macrodatos”⁸⁰. Asimismo, el “Libro Blanco sobre la inteligencia artificial —un enfoque europeo orientado a la excelencia y la confianza”⁸¹—señala específicamente que ciertas herramientas de IA de análisis facial muestran prejuicios raciales o de género. De este modo, alerta a los países miembros a ser especialmente cuidadosos y garantizar los derechos fundamentales en el uso de la IA.

3.3. Detección de denuncias falsas

Otro ámbito donde se está utilizando la IA, también objeto de controversia, es en la detección de denuncias falsas. Sobre este particular, VeriPol es una aplicación utilizada en España por el Cuerpo Nacional de Policía que procesa el lenguaje natural expresado

⁷⁸ CONSEJO EUROPEO DE PROTECCIÓN DE DATOS (2022), *passim*.

⁷⁹ PÉREZ (2021), *passim*.

⁸⁰ “Opinión de la FRA 7.4 Dado que solo un enfoque basado en derechos fundamentales garantiza un elevado nivel de protección contra el posible uso indebido de las nuevas tecnologías, los Estados miembros deberían situar los derechos fundamentales en el centro de las estrategias nacionales en materia de inteligencia artificial y macrodatos. Dichas estrategias deberían incorporar conocimientos de expertos en diversas disciplinas, como abogados, sociólogos, técnicos en estadística, informáticos y expertos en temas concretos. La ética puede ser complementaria del enfoque basado en derechos fundamentales, pero no debería sustituirlo”. Véase EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2019), pp. 165-167.

⁸¹ “Algunos programas de IA de análisis facial muestran prejuicios raciales o de género, y presentan un bajo nivel de error a la hora de determinar el género de hombres de piel más clara, pero un elevado nivel de error al determinar el género de mujeres de piel más oscura. Fuente: Joy Buolamwini, Timnit Gebru; *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81:77-91, 2018”. Véase LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza (2020), p.14.

por los denunciantes de robos con violencia y/o intimidación, lo transforma en un modelo matemático y, a partir de un aprendizaje automático, devuelve de manera inmediata una estimación de las probabilidades de que la denuncia sea falsa⁸². El programa pretende, por un lado, disuadir a los denunciantes de presentar denuncias falsas, y, por otro lado, optimizar los recursos policiales orientándolos a labores realmente necesarias. Según la información ofrecida por el Ministerio del Interior⁸³, “se trata de la primera herramienta de este tipo en el mundo y diversos experimentos empíricos demuestran que tiene una precisión superior al 90%, mientras que policías expertos alcanzan una precisión del 75%”.

Sin embargo, el uso de IA para la detección de denuncias falsas no está libre de polémica. El hecho de que un programa esté otorgando una estimación de cuán fiable es la declaración de un denunciante puede, en primer lugar, condicionar la opinión de los agentes policiales, ya que parece razonable que éstos se vean obligados a tener que justificar su opinión si ésta difiere de la del programa, y por lo tanto se muestren más propensos a adecuarse al resultado obtenido por la máquina. En segundo lugar, la estimación obtenida puede provocar que los agentes actúen con prejuicios respecto a los hechos a investigar si se ha obtenido un resultado que alumbra un nivel alto de falsedad en la denuncia y que, de esta manera, no realicen las diligencias de investigación adecuadas tendentes a la averiguación de los hechos acontecidos que podrían proporcionar resultados diferentes a los proporcionados por el programa. Y en tercer lugar, que el denunciante sea conocedor de que su declaración será puesta en duda de manera sistemática puede provocar, dependiendo de diferentes factores, como la personalidad, el estado psicológico, la confianza en el sistema de justicia, el grado de conocimiento sobre los hechos, etcétera, que éste desista de poner en conocimiento de la policía un hecho delictivo por el miedo a sentirse juzgado y no poder demostrar la veracidad de sus manifestaciones. Esto haría aumentar la ya excesivamente elevada cifra oculta de hechos delictivos producidos no denunciados, que según los datos de las encuestas de seguridad pública⁸⁴ está en aumento.

3.4. Realidad aumentada

La realidad aumentada es otro software de IA usado por los investigadores para, entre otras utilidades, reproducir la escena de un crimen. De esta manera los investigadores pueden tener una consciencia situacional del lugar dónde ha ocurrido el hecho delictivo e interactuar con él para facilitar su labor de descubrimiento del autor.

También se utilizan este tipo de aplicaciones para recrear escenas peligrosas y facilitar el entrenamiento por parte de las fuerzas y cuerpos de seguridad en situaciones que requieren un alto nivel de especialización, control y aprendizaje.

El proyecto DARLENE es un ejemplo de software de este tipo⁸⁵. Se trata de un proyecto financiado por la UE⁸⁶ que permite el procesamiento de grandes cantidades de datos, utiliza algoritmos de aprendizaje automático y proyecta construcciones tridimensionales

⁸² QUIJANO *et al.* (2018), *passim*.

⁸³ LA MONCLOA (2018), *passim*.

⁸⁴ DEPARTAMENTO DE INTERIOR DE LA GENERALITAT DE CATALUNYA (2020), *passim*.

⁸⁵ DARLENE (2022), *passim*.

⁸⁶ COMISIÓN EUROPEA (2020), *passim*.

que pone a disposición de los investigadores, para que mediante el uso de gafas de realidad aumentada puedan adentrarse en las escenas de interés para la investigación.

3.5. Drones pilotados mediante IA

El uso de drones está cobrando fuerza entre las diferentes fuerzas del orden desde hace años como herramienta para obtener imágenes de una persona sospechosa, o para acceder a un lugar difícil por motivo de su orografía o peligrosidad, o para obtener pruebas o datos de un hecho delictivo mediante la grabación de imágenes. Tradicionalmente, los drones han sido vehículos aéreos pilotados mediante control remoto desde el suelo. Actualmente, se están empleando programas de IA que son capaces de pilotar estos drones de manera autónoma, es decir sin un piloto que los controle, y que ofrecen las medidas de seguridad adecuadas para evitar colisiones.

Junto a esto, cabe señalar que se pueden incorporar otras tecnologías de IA a los propios aparatos, como por ejemplo el reconocimiento facial, la obtención de imágenes en 3D, entre otras. Otra de las ventajas del uso de drones por parte de la policía es la agilidad para la obtención de imágenes y el incremento en la visibilidad, así como un coste económico menor que el uso de otras herramientas de control aéreo, como sería la utilización de helicópteros⁸⁷. Es tal la proyección del uso de drones, que la UE está desarrollando un proyecto para la regulación del tráfico aéreo llamado U-Space⁸⁸, con la finalidad de disponer de una plataforma única de normativa y gestión del espacio aéreo de la UE.

Ahora bien, para que los datos obtenidos por un dron puedan ser empleados en el proceso penal, como no puede ser de otra manera, es imprescindible que cumplan con las debidas garantías en cuanto a la obtención de imágenes, la cadena de custodia y el acceso a ellas, con la finalidad de no colidir con los derechos fundamentales relativos a la intimidad, al secreto de las comunicaciones o a la inviolabilidad del domicilio, entre otros.

En España, las imágenes obtenidas mediante estas aeronaves teledirigidas pueden incorporarse al proceso penal al amparo del artículo 588 quinquies a) de la Ley de Enjuiciamiento Criminal, que regula la captación de imágenes en lugares o espacios público, y que establece que “La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos”.

Evidentemente, el empleo de drones no es exclusivo de las fuerzas y cuerpos de seguridad, sino que se ha generalizado y es utilizado por parte de organismos que actúan al margen de la ley, como herramienta espía, debido a las altas prestaciones que ofrecen y a su elevada discreción. Este hecho, sumado a que es difícil la identificación de los drones como herramientas policiales, genera desconfianza en la población ya que asocian su uso a posibles ataques contra la privacidad.

⁸⁷ VILLALOBOS (2020), *passim*.

⁸⁸ COMISIÓN EUROPEA (2021), *passim*.

Además, cabe señalar como otra desventaja de la utilización de los drones por parte de la policía, que éstos son fácilmente *hackeables*, por lo que hay que mejorar la tecnología para garantizar la integridad de los datos que recopilan, así como para hacerlos inmunes a los ataques que pretenden interferir entre el emisor y el receptor para inhabilitar la aeronave⁸⁹.

3.6. Ciberinvestigación masiva en la red

La tarea de ciberinvestigación en el ciberespacio, entendida como la utilización de las nuevas tecnologías de IA en la red para la averiguación del delito y el descubrimiento de su autor, una vez que se ha cometido el hecho delictivo, está provocando un cambio de paradigma en el proceso penal.

Por ello, en la fase de identificación y obtención de las evidencias será fundamental ser capaces de realizar una selección adecuada, superando las técnicas de recolección “del todo”. La fase de preservación y cadena de custodia de las evidencias requerirá disponer de los laboratorios forenses adecuados, así como usar herramientas idóneas que garanticen la inalterabilidad de las pruebas. Y finalmente, para el análisis y la realización de los informes habrá que trabajar con algoritmos *big data* y *machine learning* que sean capaces de tratar grandes volúmenes de datos, ordenarlos y reflejarlos de una manera adecuada y entendible⁹⁰.

Asimismo, cabe señalar que el uso de programas informáticos con IA en las redes por parte de las fuerzas y cuerpos de seguridad está creciendo, sobre todo para combatir el tráfico de drogas a gran escala, el terrorismo y la explotación y pornografía sexual de menores. Un ejemplo de este software es GnuWatch, desarrollado en Estados Unidos por una empresa privada en colaboración con la policía de Wyoming. Esta herramienta rastrea las redes Peer to Peer (usadas para la compartición de archivos pornográficos de menores), utiliza el número *hash* de los archivos con contenido pedófilo (dispone de un listado de miles de archivos con contenido pornográfico de menores) e identifica las direcciones IP desde donde se han compartido, accedido, publicado o descargado estos archivos. En España la Brigada de Investigación Tecnológica adscrita a la Comisaría General de Policía Judicial del Cuerpo Nacional de Policía también ha utilizado este programa para detectar con éxito a multitud de pedófilos que habían compartido y descargado este tipo de archivos. Los diferentes operativos⁹¹ comportaron la detención de los autores y la incautación de gran cantidad de material de pornografía infantil.

En Holanda, la ONG *Terre des Hommes*, que trabaja contra la explotación y los abusos sexuales a menores, creó Sweetie, una herramienta de IA diseñada como cebo para detectar a pedófilos en Internet. Sweetie es una niña virtual de 10 años, filipina, que gracias a técnicas de animación avanzadas es capaz de simular la voz, los movimientos y mantener conversaciones como si se tratara de una niña real a través de la red. Esta aplicación consiguió detectar a 20.000 pedófilos en 10 semanas, de los cuales 1.000, pertenecientes a 71 países diferentes, pudieron ser identificados, entre ellos Scott Robert Hanses, australiano, que fue el primer condenado en 2013 gracias a esta aplicación.

⁸⁹ VILLALOBOS (2020), *passim*.

⁹⁰ COSCOLLANO (2018), *passim*.

⁹¹ CENTRO CRIPTOLÓGICO NACIONAL (2011), *passim*.

La ONG pretende poner de relieve que es posible combatir el turismo sexual online, que las autoridades deben tomar medidas preventivas eficientes para proteger a la infancia de la explotación sexual, que sacar del anonimato a los depredadores sexuales online es, en numerosas ocasiones, posible, que se trata de un problema global y que para solucionarlo es necesario un enfoque novedoso, cambiar la manera de investigar y que las autoridades estén dispuestas a ello⁹².

Sweetie no está exenta de polémica, el Tribunal Correccional de Liège (Bélgica) se pronunció al respecto de esta aplicación considerando que, igual que un adulto que dice ser menor no puede considerarse menor, una niña virtual de 10 años no puede ser tenida en cuenta como una víctima menor en el sentido del artículo 379 del Código Penal belga que castiga estos ataques contra los menores⁹³. Por esta razón en 2014 se introdujo en el artículo 433 bis/1 del Código Penal belga el delito de captación de menores por Internet, para penar este tipo de conductas, reforma legislativa que también se extendió a otros países, entre ellos España.

La provocación al delito también es un punto controvertido en el uso de estos cebos en el procedimiento penal, ya que los límites de la provocación tienen que ser respetados por el avatar, de manera que es preciso que sus conversaciones sean neutras y que no inciten ni realicen alusiones sexuales. Así, los investigadores que hay detrás del avatar pueden recrear escenas cotidianas de la vida, lo cual no comportaría una provocación sino una actitud pasiva a la espera de las solicitudes espontáneas de los depredadores sexuales.

4. Derecho comparado en materia de IA

Desde hace años las instituciones de la UE (Comisión Europea, Consejo de la Unión Europea y la Agencia de Derechos Fundamentales) se han propuesto ser pioneras en la regulación normativa de la IA, con la intención de convertirse en un referente mundial en hacer compatible la transformación digital con el respeto a los derechos fundamentales respetando los valores de la Unión⁹⁴.

Ahora bien, por lo que hace referencia a investigación, desarrollo e innovación en esta tecnología, cabe señalar que la UE se ha quedado atrás en la carrera liderada por Estados Unidos y China. A continuación, se presenta el marco normativo de estas tres potencias.

4.1 Unión Europea

En 2020 la Comisión Europea publicó el “Libro Blanco⁹⁵ sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza”, como primer documento *soft law* para establecer las líneas que debía seguir la política legislativa de la UE en materia de IA.

Este Libro Blanco se basa en dos pilares: crear un “ecosistema de excelencia” en el desarrollo y aplicación de los sistemas de IA, y generar un “ecosistema de confianza” en

⁹² TERRE DES HOMMES (2013), *passim*.

⁹³ BERRENDORF (2019), *passim*.

⁹⁴ SCHUMANN (2021), p. 3.

⁹⁵ Los Libros Blancos de la Comisión Europea son documentos que contienen propuestas de acciones de la UE en un ámbito específico, con el propósito de iniciar un debate para alcanzar un consenso político con los actores implicados, el Parlamento Europeo y el Consejo de la UE.

las herramientas de IA. Para ello se plantea un enfoque basado en función del nivel de riesgo (inaceptable, alto, limitado, mínimo) que comportan los sistemas de IA, generando unas prohibiciones o limitaciones dependiendo del nivel de riesgo asignado.

Entre los sistemas clasificados de alto riesgo, se encuentra el uso de la IA para la prevención y descubrimiento del delito, dada la potencial afectación que puede generar en el ejercicio de los derechos fundamentales. Entre ellos, en el derecho a la igualdad y no discriminación (por los sesgos que pueden contener y/o perpetuar tanto los datos como los algoritmos), en el derecho a la protección de datos (alertando en especial de la vigilancia masiva biométrica y la desanonimización⁹⁶ de los datos) y en el derecho a la tutela judicial efectiva (por la opacidad de los algoritmos y la consecuente imposibilidad de impugnar sus resultados).

Después de jornadas de intensos debates en las instituciones de la Unión, el 13 de marzo de 2024 el Parlamento Europeo aprobó el Reglamento de Inteligencia Artificial⁹⁷ (en adelante AIA, por *Artificial Intelligence Act*) siguiendo las líneas marcadas en el Libro Blanco y manteniendo el enfoque basado en establecer ciertas prohibiciones u obligaciones, en función de la jerarquía de los cuatro niveles de riesgo asociado.

Por ser catalogados con un nivel de riesgo inaceptable, en dicha norma se prohíben los sistemas de IA que utilicen técnicas subliminales para distorsionar el comportamiento, así como los que exploten vulnerabilidades de un grupo específico de personas que puedan comportarle daños físicos y/o psicológicos. Asimismo, se prohíbe la elaboración de perfiles que comporte una categorización social de los individuos que pueda suponer un trato desproporcionadamente diferenciador.

En el mismo sentido, y por la injerencia que puede suponer en la libertad de reunión y en otros derechos fundamentales, se prohíbe el uso policial de la identificación biométrica en tiempo real en espacios públicos. Sin embargo, se incluyen excepciones: la búsqueda selectiva de víctimas de determinados delitos, la prevención de amenazas específicas y sustanciales contra las personas o amenazas reales o previsibles de ataques terroristas; y la localización o identificación de sospechosos de determinados delitos con un pena privativa o medida privativa de libertad superior en el Estado Miembro de más de cuatro años⁹⁸. Para llevar a cabo esta práctica será necesaria autorización judicial o

⁹⁶ La información anónima no está sometida al Reglamento de protección de datos, así queda regulado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, el cual establece en su apartado (26) que “Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.../” “...En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación”.

Sin embargo, la IA es capaz de desanonimizar la información a través del tratamiento y análisis de diferentes fuentes anónimas, e identificar a los individuos, por lo que esta técnica colidiría con el derecho a la protección de datos.

Es por este motivo, que la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece en su artículo 72.1.p) como infracción muy grave “La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados”.

⁹⁷ Resolución legislativa del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

⁹⁸ AIA, Título II “Prácticas de IA prohibidas”, artículo 5.1.d).

administrativa previa, salvo en situaciones debidamente justificadas de urgencia, en las que podrá iniciarse el uso del sistema, siempre que sin demora y en el plazo máximo de 24 horas se solicite la debida autorización a la autoridad competente⁹⁹.

El AIA clasifica como de alto riesgo aquellos sistemas de IA que pueden tener un impacto negativo en los derechos humanos¹⁰⁰. Entre ellos se encuentran los usados por las autoridades encargadas de hacer cumplir la ley para la identificación biométrica a distancia (sin perjuicio de la prohibición ya mencionada). Asimismo, también son consideradas de alto riesgo las aplicaciones de IA destinadas a la protección de infraestructuras críticas, a la evaluación del riesgo que una persona pueda ser víctima de infracciones penales, así como a la evaluación del riesgo de un individuo a delinquir o reincidir. En la misma clasificación se encuentran la utilización de polígrafos o similares, así como las herramientas de IA para la evaluación de la fiabilidad de las pruebas de una investigación o el enjuiciamiento de delitos, y la elaboración de perfiles de personas para la detección, investigación o enjuiciamiento de infracciones penales. También se incluyen en este apartado aquellos sistemas de IA destinados a ser usados por las autoridades judiciales en la investigación e interpretación de los hechos en un procedimiento.

El AIA establece unos requisitos¹⁰¹ estrictos para la IA de alto riesgo. Entre ellos, disponer de una adecuada gestión de riesgos y evaluación del impacto sobre los derechos humanos; asegurar buenas prácticas en la gobernanza y gestión de los datos que entrenan y alimentan los sistemas, evitando los sesgos discriminatorios; el registro documental de las actividades; la información a los usuarios. También se incluyen como requisitos crear un marcado CE de conformidad como garantía que el sistema cumple con los requisitos legales, la supervisión humana del sistema y los resultados, así como que los sistemas dispongan de un nivel adecuado de precisión, robustez y ciberseguridad.

Respecto a los sistemas catalogados de riesgo limitado, como los *chat-bots*, el AIA permite su uso siempre que se cumplan, entre otras, con unas obligaciones específicas de transparencia hacia los usuarios. Y finalmente, en cuanto a los sistemas que se clasifican de bajo o mínimo riesgo de afectación a los derechos fundamentales, el AIA permite su uso sin restricciones.

El ámbito de aplicación del AIA se extiende a las organizaciones no solo establecidas en la UE, sino también a aquellas que usen tecnología IA en el mercado europeo. El plazo de su entrada en vigor variará en función de la categorización del riesgo establecido. Ahora bien, en términos generales en 24 meses será plenamente aplicable. Asimismo, se crean entidades de supervisión, tales como el Comité Europeo de Inteligencia Artificial, para garantizar la correcta aplicación del AIA, así como para establecer las líneas básicas de los *sandboxes*¹⁰², con el objetivo de apoyar la innovación y el desarrollo.

⁹⁹ AIA, Título II “Prácticas de IA prohibidas”, artículo 5.3.

¹⁰⁰ AIA, Anexo III, “Sistemas de IA de alto riesgo contemplados en el artículo 6, apartado 2”.

¹⁰¹ AIA, Título III “Sistemas de IA de alto riesgo”, Capítulo 2 “Requisitos para los sistemas de IA de alto riesgo”.

¹⁰² Los *sandboxes* son entornos seguros de prueba donde poder investigar, desarrollar e innovar en un espacio controlado.

Los siete principios del AIA son “agencia y supervisión humanas; solidez y seguridad técnicas; privacidad y gobernanza de datos; transparencia; diversidad, no discriminación y equidad; bienestar social y medioambiental y responsabilidad”¹⁰³.

4.2 Estados Unidos

Estados Unidos ha tomado conciencia del carácter disruptivo de la IA y de su capacidad para cambiar la distribución del poder geoestratégico, por lo que está dedicando importantes esfuerzos a impulsar el desarrollo de la IA, sobre todo mediante financiación privada. No quiere perder su lugar como potencia mundial en favor de otras potencias que están emergiendo con fuerza en esta materia, como China.

Si bien Estados Unidos no ha establecido todavía un marco legal en materia de IA, la Administración Biden parece haber tomado conciencia de los posibles efectos negativos de su uso indiscriminado y ha incluido dentro de su estrategia nacional la publicación del Proyecto de Declaración de Derechos sobre la IA (*Blueprint for an AI Bill of rights*¹⁰⁴) y el manual que lo acompaña *From Principles to Practice*¹⁰⁵ para el impulso y desarrollo de la IA.

Se establecen cinco principios que deberán regir la creación, el desarrollo y la implementación de sistemas de IA, que se enumeran a continuación¹⁰⁶:

1. Sistemas seguros y eficaces: será indispensable que se identifiquen los riesgos que pueden generar para los diferentes ámbitos en los que se apliquen, tendrán que pasar las debidas evaluaciones previas a su implementación, así como auditorías periódicas, y únicamente podrán utilizar los datos que sean imprescindibles para sus fines.
2. Protección contra la discriminación algorítmica: será necesario evitar que los sistemas arrojen resultados discriminatorios por razón de raza, color, origen, sexo, y otros. Para ello, será preciso realizar evaluaciones periódicas para comprobar que no se están produciendo desviaciones.
3. Privacidad de los datos: se deberán evitar las prácticas abusivas, los datos tienen que usarse para la finalidad que fueron recogidos y con el debido consentimiento informado.
4. Aviso y explicación: será obligatorio explicar en un lenguaje comprensible el funcionamiento del sistema, así como las repercusiones para la persona afectada.
5. Intervención humana, valoración e impugnación de la decisión: las decisiones tomadas de manera automática han de poder ser impugnadas y reconsideradas delante de un humano.

El Proyecto de Declaración de Derechos sobre la IA no dispone de respaldo legislativo. Además, tampoco goza del beneplácito de la Cámara de Comercio estadounidense, que

¹⁰³ AIA, consideración 14 bis.

¹⁰⁴ THE WHITE HOUSE (2023), *passim*.

¹⁰⁵ THE WHITE HOUSE (2022), *passim*.

¹⁰⁶ BARADAT (2023), *passim*.

pone en duda la competitividad de sus empresas en el caso de que los legisladores promulgasen el proyecto como reglas¹⁰⁷.

4.3 China

Por su parte, el Ministerio de Ciencia y Tecnología de China publicó en octubre de 2021 un código ético para regular los sistemas de IA denominado “Especificaciones Éticas para Inteligencias Artificiales de Nueva Generación”¹⁰⁸. Se enfoca en controlar las transformaciones sociales que provocarán los sistemas de IA, poniendo el acento en proteger los derechos de los usuarios para controlar la influencia en la alineación social, asegurándose de que la IA está en todo momento bajo control humano y que es este quien tiene el pleno poder de decisión. Dicho documento recoge como principios básicos que los sistemas sean controlables y confiables; que mejoren el bienestar humano; que promuevan la equidad, la transparencia y la justicia; que protejan la privacidad y la seguridad; y aumenten la educación ética.

En abril de 2023, la Administración China publicó un borrador con las normas reguladoras que estarán obligados a seguir los desarrolladores de sistemas de IA¹⁰⁹, según las cuales se creará un registro de identificación de todos los usuarios para tener un control exhaustivo de su uso. Además, se establece que “el contenido generado por la inteligencia artificial generativa debe encarnar los valores socialistas fundamentales y no debe contener ningún contenido que subvierta el poder estatal, abogue por el derrocamiento del sistema socialista, incite a la división del país o socave la unidad nacional”.

China, en consonancia con su política de control exhaustivo de su población, se ha propuesto controlar la influencia de las empresas tecnológicas sobre su ciudadanía, así como convertirse en líder mundial en IA en 2030.

5. Conclusiones

La irrupción de la IA en el ámbito policial constituye un importante desafío tecnológico y jurídico. Por ello, este trabajo aborda los usos concretos de la IA tanto en la fase preventiva, como en la fase investigativa del delito, compara los primeros modelos normativos internacionales e identifica los riesgos asociados, proponiendo criterios éticos y regulatorios para una aplicación respetuosa con los derechos fundamentales.

Con base a estos objetivos, puede concluirse que el uso de la IA en la prevención e investigación criminal debe abordarse desde un enfoque antropocéntrico. La IA debe ser un instrumento al servicio de las personas que ayude a las fuerzas y cuerpos de seguridad a ser más efectivos y eficientes en la orientación de los servicios policiales para prevenir e investigar el delito.

La aplicación de la IA en la prevención delincriminal debe ir acompañada de la apertura de un debate social sobre las injerencias en la privacidad que estamos dispuestos a asumir para aumentar la detección de los delitos antes de que se produzcan. Asimismo, es necesario someter a discusión los modelos algorítmicos que se utilicen para garantizar que están en consonancia con la ética de las sociedades democráticas del siglo XXI. Los

¹⁰⁷ IGLESIAS (2022), *passim*.

¹⁰⁸ SHEN (2021), *passim*.

¹⁰⁹ BIURRUN (2023), *passim*.

consensos a los que se llegue deben ser reflejados en una regulación normativa “preprocesal” que dé seguridad jurídica tanto a los ciudadanos, como a la policía en sus tareas de prevención del delito mediante el uso de IA. Por ello, será imprescindible delimitar de manera adecuada dónde situar la línea entre las labores preventivas asistidas por IA y las investigaciones prospectivas, vedadas por la doctrina y la jurisprudencia.

Por lo que respecta al uso de la IA en la investigación criminal, se debe velar por que la actual sobreexposición de los usuarios en las redes sociales no conlleve una laxitud de las garantías procesales. Asimismo, cabe tomar en consideración que los sistemas de reconocimiento de patrones biométricos, tanto en espacios físicos, como en espacios cibernéticos, así como la ciberinvestigación y las otras herramientas de IA utilizadas en este ámbito, pueden ayudar de manera significativa a las labores de investigación policial. Ahora bien, no se puede obviar que estos instrumentos suponen no solo una profunda intrusión en la intimidad de las personas, sino que además pueden comportar prejuicios raciales, ideológicos y perpetuar sesgos discriminatorios. Por lo tanto, los resultados arrojados por estos sistemas deberán ser supervisados por los investigadores y corroborados por las otras diligencias de investigación que se puedan practicar para garantizar su precisión y robustez.

Otro aspecto esencial en la aplicación de la IA a la prevención e investigación del delito es la necesidad que las Administraciones Públicas realicen las inversiones en recursos, innovación, investigación, desarrollo y formación. Solo a través de una estrategia pública sólida y sostenible será posible fortalecer la capacidad tecnológica del sector público y garantizar, con ello, el respeto efectivo de los derechos fundamentales. En consecuencia, no resulta aceptable delegar en grandes corporaciones tecnológicas —guiadas por intereses privados— la gestión de los datos personales, ni el diseño, desarrollo y supervisión de los sistemas de IA destinados a la función policial.

Para ello, será necesario definir un marco de gobernanza de desarrollo y aplicación de estas tecnologías con consenso a nivel global, dado que su impacto trasciende los límites de la territorialidad. El crimen organizado ya está haciendo uso de la IA para mejorar y optimizar los beneficios de su actividad criminal. Por lo tanto, es necesario establecer una legislación transfronteriza que impida la existencia de espacios de impunidad digital que imposibiliten la persecución del delito. Asimismo, cabrá dotar a las fuerzas del orden de tecnología avanzada y formación adecuada para que sean capaces de combatir la criminalidad con sus propias armas.

Las políticas criminales en materia de IA deben huir de la monitorización de los ciudadanos como garantía de seguridad. La categorización de las personas promovida por los sistemas de IA puede aumentar las desigualdades sociales, coartar la enriquecedora diversidad cultural y alimentar actitudes de exclusión hacia quienes se apartan de los modelos dominantes, contribuyendo a acentuar la polarización y conflictividad social.

En síntesis, la aplicación de la IA en las funciones policiales plantea un reto que consiste en aprovechar su potencial sin comprometer los derechos fundamentales, ni la integridad del proceso penal. La IA debe orientarse como un instrumento al servicio de las personas que responda a valores éticos, transparencia y supervisión humana efectiva. Resulta esencial regular sus usos en la prevención e investigación del delito, garantizar la rendición de cuentas y evitar la dependencia tecnológica del sector público respecto de intereses privados.

Finalmente, y teniendo en cuenta la emergencia medioambiental en la que vivimos, se debe valorar la huella ecológica que generan los sistemas de IA y promover los algoritmos “verdes” basados en una economía digital reutilizable respetuosa con el entorno natural.

Bibliografía citada

- ANGWIN, Julia; LARSON, Jeff; KIRCHNER, Lauren; MATTU, Surya: “Machine Bias”. Disponible en: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [visitado el 25/10/2025].
- ARENAS GARCÍA, Lorea (2017): “Los medios de control telemático en el sistema penal español”, en: Repositorio Institucional de la Universidad de Málaga.
- BARADAT, Ramón (2023): “Estados Unidos lanza un catálogo de principios en materia de Inteligencia Artificial”, en: Cuatrecasas. Disponible en: <https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/estados-unidos-lanza-un-catalogo-de-principios-en-materia-de-inteligencia-artificial> [visitado el 25/10/2025].
- BARONA VILAR, Silvia (2019): “Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia”, en: Revista Jurídica Digital UANDES (Vol. 3, nº 1), pp. 1-17.
- BECK, Ulrich (2019): La sociedad del riesgo. Hacia una nueva modernidad. (Trad. Jorge Navarro, Daniel Jiménez, M^a Rosa Borrás, Buenos Aires, Paidós).
- BERRENDORF, Alyson; ROYER, Sofie (2019): “Le droit pénal belge face à l’intelligence artificielle: de l’appréhension par le droit pénal belge d’un avatar”, en: Revue de Jurisprudence de Liège, Mons et Bruxelles, (nº 14), pp. 644-653.
- BIURRUN, Alfredo (2023): “China regula que sus modelos de inteligencia artificial tengan “valores socialistas””, en La Razón. Disponible en: https://www.larazon.es/tecnologia/china-regula-que-sus-modelos-inteligencia-artificial-tengan-valores-socialistas_202304126435c98d1b5f5b00013fe995.html [visitado el 25/10/2025].
- CAMPIONE, Roger (2020): “La plausibilidad del derecho en la era de la inteligencia artificial: filosofía carbónica y filosofía silícica del derecho”, en: Sociología y Tecnociencia (Vol. 11, nº2), pp. 123-139.
- CENTRO CRIPTOLÓGICO NACIONAL (2011): “GNUWATCH, la nueva herramienta forense de la Policía Nacional ha permitido detener a 10 pedófilos”. Disponible en: <https://www.ccn-cert.cni.es/en/updated-security/warnings-ccn-cert/911-gnuwatch-la-nueva-herramienta-forense-de-la-policia-nacional-ha-permitido-detener-a-10-pedofilos.html> [visitado el 25/10/2025].
- COMISIÓN EUROPEA (2020): “Realidad aumentada para ayudar a las fuerzas de seguridad a combatir la delincuencia”. Disponible en: <https://cordis.europa.eu/project/id/883297/es> [visitado el 25/10/2025].
- COMISIÓN EUROPEA (2021): “Plan móvil 2021 para la normalización de las TIC”. Disponible en: <https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/u-space> [visitado el 25/10/2025].
- COMISIÓN EUROPEA (2021): “Periodic Reporting for period 2 – IborderCtrl (Intelligent Portable Border Control System)”. Disponible en: <https://cordis.europa.eu/project/id/700626/reporting> [visitado el 25/10/2025].
- COMISIÓN EUROPEA (2023): “Ponerse al día con VALCRI: aprovechar los macrodatos para luchar con éxito contra la delincuencia”. Disponible en: <https://cordis.europa.eu/article/id/124663-catching-up-with-valcri-harnessing-big-data-to-successfully-fight-crime> [visitado el 25/10/2025].
- COMISIÓN EUROPEA (2023): “Actualización sobre VALCRI: utilización de datos masivos para luchas de forma eficaz contra la delincuencia”. Disponible en:

- <https://cordis.europa.eu/article/id/124663-catching-up-with-valcri-harnessing-big-data-to-successfully-fight-crime/es> [visitado el 25/10/2025].
- CONSEJO EUROPEO DE PROTECCIÓN DE DATOS (2022): “Facial recognition: Italian SA fines Clearview AI EUR 20 million”. Disponible en: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en [visitado el 25/10/2025].
- COSCOLLANO, Carlos (2018): “Evolución tecnológica y datos: ¿nuevo paradigma para ‘forensic digital’ y ciberinvestigaciones?”, en: *Redseguridad* (nº82), pp. 38-39.
- DARLENE (2022): “Ecosistema de aplicación de la ley de RA profunda”. Disponible en: <https://www.darleneproject.eu/> [visitado el 25/10/2025].
- DEPARTAMENTO DE INTERIOR DE LA GENERALITAT DE CATALUNYA (2020): “Informe 2020 sobre la Seguridad en Cataluña. Departamento de Interior de la Generalitat de Catalunya”. Disponible en: https://interior.gencat.cat/web/.content/home/010_el_departament/publicacions/seguretat/estudis_i_enquestes/informes_de_seguretat/informes_de_seguretat/02_I_SC-2020-2022-07-12_ES.pdf [visitado el 25/10/2025].
- ESTÉVEZ MENDOZA, Lucana María (2020): “Inteligencia artificial y violencia contra las mujeres: ¿funcionan los sistemas automatizados de evaluación del riesgo?”, en: *Perspectivas*, (nº3), pp. 127-141.
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2019): “Fundamental rights report 2019”. Disponible en: <https://fra.europa.eu/en/publication/2019/fundamental-rights-report-2019> [visitado el 25/10/2025].
- FERNÁNDEZ RODRÍGUEZ, José Julio (2019): “El encuentro entre seguridad y derechos humanos: actualidad y problemas”, en: *Revista de Relaciones Internacionales, Estrategia y Seguridad*, (Vol.14, nº 1), pp. 87-101.
- FREIRE MONTERO, Antón Fructuoso (2022): “El reconocimiento facial como instrumento de investigación y prevención del delito”, en: *Anuario da Facultade de Dereito da Universidade da Coruña*, (nº 26), pp. 64-88.
- GARCÍA TORRES, María Luisa (2025): “Judicial Administration 4.0: strengths, challenges and opportunities of a proactive approach to AI regulation in Spain”, en: *TalTech Journal of European Studies*, (Vol.15, nº1), pp- 106-134.
- GARTLAND, Claire (2016): “Biometrics Are a Grave Threat to Privacy”, en: *The New York Times*, en la sección *The Opinion Pages*. Disponible en: <https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy> [visitado el 25/10/2025].
- GARVIE, Clare; BEDOYA, Álvaro; FRANKLE, Jonathan (2016): “The perpetual line-up: Unregulated police face recognition in America”. Disponible en: <https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/> [visitado el 25/10/2025].
- GILETTA, Matías; GIORDANO, Ariel; MERCAÚ, Noelia; ORDEN, Pedro; VILLAREAL, Vanesa (2020): “Inteligencia Artificial: definiciones en disputa”, en: *Sociales Investiga* (nº9), pp. 20-33.
- GÓMEZ COLOMER, Juan Luís (2023): *El juez robot: la independencia judicial en peligro*. (Valencia, Tirant lo Blanch).
- GONZÁLEZ ÁLVAREZ, José Luis; LÓPEZ OSSORIO, Juan José; MUÑOZ RIVAS, Marina (2018): “La valoración policial del riesgo de violencia contra la mujer pareja en España–Sistema VioGén.”, en: *Ministerio del Interior, Gobierno de España*.

- GONZÁLEZ ÁLVAREZ, José Luís; SANTOS HERMOSO, Jorge; CAMACHO COLLADOS, Miguel (2020): “Policía predictiva en España. Aplicación y retos futuros”, en: Behavior & Law Journal (Vol. 6, nº 1), pp. 26-41.
- GREENE, Jack (2006): “La policía de proximidad en Estados Unidos: cambios en la naturaleza, estructura y funciones de la policía”, en: Justicia Penal del Siglo XXI, pp. 349-424.
- HAO, Karen (2021): “Caso práctico: probamos por qué un algoritmo judicial justo es imposible” (Trad. Ana Milutinovic). Disponible en: <https://technologyreview.es/article/caso-practico-probamos-por-que-un-algoritmo-judicial-justo-es-imposible/> [visitado el 25/10/2025].
- HERNÁNDEZ GIMÉNEZ, Maria (2019): “Inteligencia artificial y derecho penal”, en : Actualidad jurídica iberoamericana (nº 10), pp. 792-843.
- HOLLOWAY, David (2008): “9/11 and the War of Terror” (Edimburgo, Edinburgh University Press).
- IGLESIAS ÁLVAREZ, Irene (2022): “La Administración Biden despliega un plan propio sobre inteligencia artificial”, en: IDG Communications S.A.U. Disponible en: <https://www.computerworld.es/article/2113650/la-administracion-biden-despliega-un-plan-propio-sobre-inteligencia-artificial.html> [visitado el 25/10/2025].
- INTERPOL (2024): “Bases de datos”. Disponible en: <https://www.interpol.int/es/Como-trabajamos/Bases-de-datos> [visitado el 25/10/2025].
- LA MONCLOA (2018): “La Policía Nacional pone en funcionamiento la aplicación informática VeriPol para detectar denuncias falsas”. Disponible en: <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2018/271018veripol.aspx> [visitado el 25/10/2025].
- LIN, Liza; NEWLEY, Purnell (2019): “A World With a Billion Cameras Watching You Is Just Around the Corner”, en The Wall Street Journal.
- MARTÍN RÍOS, Pilar (2022): “Empleo de ‘big data’ y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras”, en: IDP. Revista de Internet, Derecho y Política, (36), pp. 1-13.
- MINISTERIO DE IGUALDAD, GOBIERNO DE ESPAÑA (2024): “Ficha estadística de víctimas mortales por Violencia de Género”. Disponible en: <https://violenciagenero.igualdad.gob.es/violenciaencifras/victimasmortales/ficha-mujeres/> [visitado el 25/10/2025].
- MINISTERIO DE IGUALDAD, GOBIERNO DE ESPAÑA (2024): “Ficha estadística de menores de edad víctimas mortales en casos de Violencia de Género contra su madre”. Disponible en: <https://violenciagenero.igualdad.gob.es/violenciaencifras/victimasmortales/ficha-menores/> [visitado el 25/10/2025].
- MIRÓ LLINARES, Fernando (2018): “Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots”, en: Revista de Derecho Penal y Criminología (nº 20), pp. 87-130.
- MONTESINOS GARCÍA, Ana (2021): “Los algoritmos que valoran el riesgo de reincidencia: En especial, el sistema Viogen”, en: Revista de derecho y proceso penal (nº 64), pp. 19-55.
- OLIVA LEÓN, Ricardo (2022): “¿Justicia algorítmica ética? Algoritmo Legal”. Disponible en: <https://www.algoritmolegal.com/tecnologias-disruptivas/justicia-algoritmica-etica/> [visitado el 25/10/2025].
- OTERO GONZÁLEZ, María del Pilar (2008): Control telemático de penados : análisis jurídico, económico y social (Valencia, Tirant lo Blanc).

- PASTORINI, Joselina (2020): “Prevención y persecución de ciberdelitos: ¿un nuevo terreno para la inteligencia artificial?”, en: *Revista Internacional de Derecho Público* (n°4), pp. 92-99.
- PÉREZ ESTRADA, Miren Josune (2021): “La inteligencia artificial como prueba científica en el proceso penal español”, en: *Revista Brasileira de Direito Processual Penal* (Vol. 7, n° 2), pp. 1385-1385.
- PLANCHADELL GARGALLO, Andrea (2021): “Inteligencia Artificial y medidas cautelares”, en: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, pp. 389-419.
- PLANCHADELL GARGALLO, Andrea (2023): “Víctimas de trata de seres humanos, investigación del delito y nuevas tecnologías”, en: *El proceso penal ante una nueva realidad tecnológica europea*, pp. 393-412.
- QUIJANO SÁNCHEZ, Lara; LIBERADOS, Federico; CAMACHO COLLADOS, José; CAMACHO COLLADOS, Miguel (2018): “Aplicación de detección automática basada en texto de lenguaje engañoso a informes policiales: extracción de patrones de comportamiento de un modelo de clasificación de varios pasos para comprender cómo mentimos a la policía”, en: *Sistemas basados en el conocimiento* (n° 149), pp. 155-168.
- RIQUELME, José Cristobal; RUIZ, Roberto; GILBERT, Karina (2006): “Minería de Datos: Conceptos y Tendencias”, en: *Revista Iberoamericana de Inteligencia Artificial* (Vol. 10, n° 29), pp. 11-18.
- ROA AVELLA, Marcela del Pilar; SANABRIA MOYANO, Jesús Eduardo; DINAS HURTADO Katherin (2022): “Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos”, en: *Revista Brasileira de Direito Processual Penal* (n° 8), pp. 275-310.
- SÁNCHEZ MONEDERO, Javier; DENCİK, Lina (2020): “The Politics of Deceptive Borders: ‘Biomarkers of Deceit’ and the Case of iBorderCtrl”, en: *Information, Communication & Society* (Vol. 25, n°3), pp. 413-430.
- SCHUMANN BARRAGAN, Guillermo (2021): “La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE”, en: *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, pp. 517-539.
- SHEN, Xin Mei (2021): “Chinese AI gets ethical guidelines for the first time, aligning with Beijing’s goal of reining in Big Tech”, en: *South China Morning Post*. Disponible en: <https://www.scmp.com/tech/big-tech/article/3150789/chinese-ai-gets-ethical-guidelines-first-time-aligning-beijings-goal> [visitado el 25/10/2025].
- SOUZA DE MENEZES, Cyntia; AGUSTINA, José R. (2020): “Big data, inteligencia artificial y policía predictiva: bases para una adecuada regulación legal que respete los derechos fundamentales”, en: *Cibercrimen III: inteligencia artificial, automatización, algoritmos y predicciones en el derecho penal y procesal penal*, p. 137-181.
- RODRÍGUEZ FERNÁNDEZ, Ricardo (2022): “El juez sentenciador y la inteligencia artificial (a propósito del ingreso de Manuel Marchena como Académico de Número en la Real Academia de Doctores)”, en: *Diario La Ley* (n° 10184), p. 3.
- TAVORA SERRA, Manuel (2023): “Ciberpatrullaje en el medio virtual. Delimitando conceptos”, en: *Ius et Scientia* (Vol. 9, n° 1), pp. 81-97.
- TERRE DES HOMMES (2013): “La niña virtual Sweetie, creada por Tierra de hombres en Holanda, consigue identificar a más de 1000 pedófilos de 65 países”. Disponible en: <https://tdh.tierradehombres.org/la-nina-virtual-sweetie-creada-por-tierra-de-hombres-en-holanda-consigue-identificar-pedofilos-ayuda-infancia/> [visitado el 25/10/2025].

- THE WHITE HOUSE (2022): “From Principles to Practice | OSTP | The White House”.
- THE WHITE HOUSE (2023): “Blueprint for an AI Bill of Rights | OSTP | The White House”.
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2023): “La población mundial sin conexión sigue disminuyendo hasta los 2.600 millones de personas en 2023”. Disponible en: <https://www.itu.int/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx> [visitado el 25/10/2025].
- UNITED STATES DEPARTMENT OF HOMELAND SECURITY (2014): “Future Attribute Screening Technology”, en DHS Science and Technology Directorate. Disponible en: <https://www.dhs.gov/archive/publication/future-attribute-screening-technology> [visitado el 25/10/2025].
- VAAK (2023): “IA de análisis de cámaras de seguridad que admite DX”, Disponible en: <https://vaak.co/> [visitado el 25/10/2025].
- VILLACAMPA ESTIARTE, Carolina; GÓMEZ ADILLÓN María Jesús (2016): “Nuevas tecnologías y victimización sexual de menores por online grooming”, en: Revista electrónica de ciencia penal y criminología (nº 18), pp. 1-27.
- VILLALOBOS FONSECA, Hazel (2020): “El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito”, en: Revista de Relaciones Internacionales, Estrategia y Seguridad (Vol. 15, nº 1), 79-97.

Jurisprudencia citada:

- Estados Unidos: Corte Suprema de Wisconsin, State v. Loomis, 881 N.W.2d 749 (2016).
- Países Bajos: Corte de Distrito de La Haya, ECLI:NL:RBDHA:2020:1878 (2020).
- España: SAN 2350/2020.
- España: STS 1119/2025.