

Herramientas de inteligencia artificial en la investigación policial: cuestiones legales



Eloy Velasco Núñez

Magistrado-Juez de la Audiencia Nacional

1.- Tipología y herramientas ia de investigación policial:

Acorde con la definición de los sistemas de Inteligencia Artificial recogida en el artículo 3.1 del Reglamento (UE) 2024/1689 de Inteligencia Artificial —en adelante RIA—, la magnitud y diversidad de técnicas que incorpora¹, de seguro, darán con múltiples aplicaciones y herramientas² que, sin duda, podrán usarse —se está haciendo ya—, como en muchos otros campos profesionales,

también en la investigación policial de delitos.

Así, y a título meramente enunciativo, habrá herramientas de IA generativa que la investigación policial destinará a responder consultas; aportar estrategias sobre la base de casos previos; encauzar primeras fases de estudio; hacer planteamientos iniciales en asuntos replicables; y asistir en la confección de borradores, o primeras aproximaciones documentales.

Otras aplicarán la automatización pura, total o parcial, de tareas y procesos (RPA³), con el fin de anotar la entrada, registro y reparto de asuntos —búsqueda de atestados, informes, vigilancias—; aplicar buscadores de pericias; recuperar información; operar como redactores y montadores de documentos o textos sobre modelos previos; realizar análisis documental mediante resumen, clasificación, detección, transcripción o sugerencia de respuesta; clasificar materias y optimizar recursos.

Igualmente habrá herramientas destinadas a llevar a cabo la gestión de procesos⁴: aportando información sobre el estado de una investigación y cómo va el asunto en tiempo real; exhibiendo el mapa del asunto; generando recomendaciones o predicciones para la conformación de la estrategia; activando sistemas de avisos o alertas, como supervisión de hitos o plazos de prescripción; llevando a cabo notificaciones; optimizando preguntas y buscando información concreta para resolver el asunto; asistiendo a la tramitación —pericias, reconocimiento de voz, hallazgo de piezas de convicción, reconstrucción de hechos, detección y rastreo de operaciones sospechosas—; operando chatbots de información y relación con el público; ayudando a la preparación previa de citas telemáticas; textualizando grabaciones; traduciendo o interpretando, incluso simultáneamente; confeccionando citas previas, o auxiliando en tareas de mediación.

Ítem más, la IA ayudará asistencialmente y con apoyo matemático al análisis de numerosos

1 Estrategias técnicas de propósito genérico y de propósito específico, de aprendizaje, lógica y conocimiento y estadísticas

2 “Casos de uso”, según la terminología utilizada por los ingenieros informáticos.

3 Robotic Process Automation. Aunque se indique que la automatización de tareas no tiene por qué ser IA, dada su normal falta de autonomía, al tratarse de auténticos algoritmos en procesos de ordenación, el hecho de que inferan resultados de salida se le semeja y sirve a nuestros fines.

4 La investigación policial, en sí, es un proceso más o menos largo gestionado por sus artífices. Secretario, instructor, responsable, partícipe, etc.

datos, a inferir y contribuir en el proceso de toma de ciertas decisiones de avance en la investigación policial —herramientas asistentes a toma de decisiones— mediante los oportunos árboles de decisión, en asuntos como la asistencia para la argumentación; la evaluación de la solidez de los diferentes medios de prueba, donde habrá que abrir, desde otra nueva perspectiva valorativa, si los medidores de datos corporales del interrogado, como polígrafos y detectores de cambios de comportamiento en los denominados “detectores de mentiras” en pruebas personales, tienen o no validez convictiva legal; o la asistencia a decisiones basadas en probabilidades y riesgos de predicción —impago, fuga, reiteración, ocultación de pruebas— y alertas tempranas.

Desde otro punto de vista clasificatorio, podremos analizar la coexistencia de herramientas que incorporen estrategias de propósito específico en el apoyo a la investigación policial basadas en lo que podríamos denominar IA tradicional (ML), estrategia técnica que resuelve problemas concretos aprendiendo de datos pasados para clasificar, predecir o decidir; esto es, que no inventa ni innova, sino que reconoce patrones de los que infiere sus prácticos resultados de salida.

Estamos refiriéndonos a motores de recomendación; sistemas de predicción —v. gr.: Compas, que predice el posible riesgo de fuga de personas penadas por

la ley—; y sistemas de reconocimiento automático en el análisis de anomalías en pautas de comportamiento, tan aplicados ya para la detección y, en su caso, supresión de intentos de fraude en tiempo real. Herramientas de propósito específico óptimas para predecir comportamientos futuros basados en datos históricos —v. gr.: posible consumo de droga—; detectar anomalías o clasificar información precisa; optimizar procesos para ganar eficiencia; emplearse en entornos críticos fiables y precisos —v. gr.: finanzas—, y apoyar decisiones basadas en datos reales.

Enfrente de ellas, las herramientas de propósito general, con empleo de la denominada IA generativa, analizan y generan a partir de los datos con que entrenan, llegando a crear, personalizar e interactuar con resultados útiles en la investigación policial. Ejemplos de su aplicación podrían ser la creación de texto a partir de ideas; la generación de elementos visuales —gráficos o dibujos— sacados de una descripción escrita; o la confesión de borradores, prototipos y escenarios desde patrones aprendidos.

Los casos de uso de esta IA generativa son buenos para crear contenido —texto o imagen, v. gr.: hacer un retrato robot de la posible imagen de un sospecho sobre los datos aportados por testigos presenciales—; experimentar o explorar escenarios —para diseñar productos que utilizar el día de reviente de una investigación—; interactuar con

usuarios —chatbots, asistentes e interfaces conversacionales para ayudar a posibles víctimas de violencia doméstica—; personalizar mensajes en las aportaciones de afectados por algún tipo concreto de delito —v. gr.: VioGén—; y simular escenarios con escasos datos reales entrenables, ayudándose de infografías para entrenar la posible escena de crímenes importantes o de criminalidad organizada y escenarios complejos asociados, como rutas de fuga o llegada a la escena del crimen.

Y como señala BENAVENTE⁵, no se trata de enfrentar preferencias entre una especie de IA, la tradicional, u otra, la generativa, sino de combinar ambas mediante soluciones híbridas que integren y complementen ambos enfoques, como ya se está realizando con muchas herramientas en el mercado de la investigación policial.

En el campo práctico encontramos herramientas que llevan a cabo búsquedas de hashes⁶ delictivos acreditados; usan patrones matemáticos únicos para su detección; o emplean técnicas de filtrado de información que sirven para escanear o monitorear contenidos aprendidos a sospechosos criminales por presunta actividad delictiva concreteable —imágenes, vídeos, datos de tráfico—, muy útiles en el análisis de documentación electrónica intervenida; por ejemplo, en dispositivos técnicos asociados a un sospechoso tras un registro domiciliario o una detención. Allí,

5 BENAVENTE, Juan, “IA tradicional vs IA generativa: entendiendo sus diferencias. <https://datos.gob.es>. 16/09/2025.

6 Resúmenes algorítmicos de cuerpos delictivos tecnológicos (fraudes, materiales de abuso sexual infantil, etc.) ya detectados en el pasado, a veces incluso castigados, que pueden seguir difundiendo o empleando nuevos partícipes delictivos.

la búsqueda de coincidencias de hashes —huellas digitales— respecto de previos cuerpos delictivos digitales, v. gr.: casos ya castigados o investigados de fraude o posesión de material pornográfico infantil, permite contrastar y comparar, y si da un “match”⁷, la información asociada, incluidas direcciones IP vinculadas a esos archivos, puede fundar claras imputaciones concretas a investigados muy precisos.

Otras herramientas emplean clasificadores o analizadores de pautas de comportamiento digital, clasificadores de aprendizaje automático que aplican sobre vídeos —v. gr.: CSAI Match de Yahoo/Google— o fotos estáticas —API de Facebook—, incluso no vistas, inéditas o desconocidas. También pueden operar sobre listas de reproducción, miniaturas y comentarios en redes sociales que sexualizan menores, para detectar presuntos depredadores sexuales, permitiendo restringir funciones en directo, como inhabilitar comentarios o limitar recomendaciones del vídeo afectado, minorando el alcance buscado por el sospechoso.

Los anteriores, combinados con algoritmos de análisis documental, masivo de datos y metadatos, pueden ser muy útiles en el escaneo e investigación de la escena de un crimen o, con el oportuno mandamiento judicial, del ámbito digitalmente documentado de la privacidad de un sospechoso; o, en delitos económicos, especialmente blanqueo de activos, en el escaneo para la detección de

posibles operaciones sospechosas o inexplicables.

Más conocidas y tratadas son las herramientas fundadas en técnicas de reconocimiento —lenguaje natural, audio, biométrico y facial— de la voz o la imagen de un sospechoso para la imputación participativa en delitos que han dejado rastros fisiológicos de esa naturaleza. Cuando no el empleo de ataques adversariales para engañar a IAs delictivas y abortarlas, dentro de instrumentos predictivos y evitativos de delitos, muy útiles frente a quienes utilizan fakes y reclamos fraudulentos para delinquir contra víctimas, tanto en delincuencia económica como terrorista o sexual, especialmente frente a víctimas vulnerables.

2.- Marco legal y garantías jurídicas que deben observar las herramientas policiales de ia en la investigación delictiva:

Desde una perspectiva legal, conviene recordar que, para diferenciarse del delincuente que combate, el Estado de Derecho somete la actuación de quienes contribuyen a la declaración de lo que es o no delito —jueces, fiscales, cuerpos policiales y ciudadanos particulares cuando la ley se lo permite a través de sus abogados— a reglas éticas encuadrables en las normas de exclusión probatoria, cuando la obtención de las evidencias afecta a derechos fundamentales —art. 11.1 LOPJ—.

Traídas al campo de las herramientas IA que analizamos, es todavía escaso el marco legal que las define. Destaca, no obstante, el voluntario RIA, que al definir en su artículo 5 determinadas aplicaciones IA prohibidas —tecnología prohibida por el altísimo riesgo dañino y la enorme afectación negativa en derechos fundamentales— convierte las inferencias acusatorias deducidas por ciertas herramientas IA en técnicas prohibidas que, procesalmente, el juez no puede considerar para probar delitos, dado su riesgo inaceptable. Así ocurre con aquellas que:

1. Alteren de manera sustancial el comportamiento explotando vulnerabilidades de personas físicas o colectivos por razón de edad, discapacidad o situación social o económica.
2. Evalúen o clasifiquen personas físicas o colectivos por su comportamiento social o determinadas características de personalidad, generándoles un trato perjudicial desproporcionado.
3. Evalúen riesgos de personas físicas para predecir el riesgo de delito si se basan en rasgos y conductas de su personalidad.
4. Utilicen bases de reconocimiento facial extraídas de Internet o de circuitos cerrados para inferir emociones en el trabajo o centro escolar, salvo motivo médico o de seguridad.

⁷ Coincidencia de hashes.

5. Usen sistemas de identificación biométrica⁸ remota en tiempo real en espacios de acceso público, salvo casos de víctimas de trata, delitos sexuales, secuestros, desaparecidos, terrorismo, o localización de sospechosos, etc., conforme al anexo y siempre con cobertura legal nacional⁹, y pena máxima de al menos cuatro años de prisión.

E igualmente habrá de observarse toda la normativa de desarrollo y garantías que el RIA anuda a los sistemas de alto riesgo, como son los aquí estudiados para la investigación policial por su relación con la Administración de Justicia y la aplicación del Derecho afectando a derechos fundamentales.

Al margen de lo anterior, nos encontramos en una incipientísima época en la que el sometimiento de estas herramientas de IA a la legalidad se mueve también, a falta de leyes más precisas, en la aplicación jurisprudencial de principios jurídicos que tales herramientas deben observar, entre los que cabe enunciar, para terminar, los siguientes:

1. Interdicción de la discriminación mediante inferencias de sesgo, de cara a potenciar el principio de igualdad.
2. Prohibición de la opacidad, potenciando transparencia y explicabilidad en la adopción de decisiones asistidas con IA, incluidos árboles de decisión y códigos fuente abiertos¹⁰.

3. Interdicción de la cosificación humana mediante el principio de humanización, resumido en que las decisiones sean, en último grado, asumidas con supervisión humana —art. 22 RGPD—, y no exclusivamente mediante tratamiento automatizado.
4. Interdicción del ataque, directo o indirecto, a derechos fundamentales —art. 11.1 LOPJ—.
5. Limitación del tratamiento, mediante atribución a una finalidad lícita y legal, y minimización de datos —art. 5.1.c RGPD—.

⁸ Biológicos/conductuales que identifican unívocamente a una persona.

⁹ En el caso español, tal noma legal de cobertura y desarrollo del Art. 5.5 RIA, todavía no se ha aprobado a fecha mayo de 2026.

¹⁰ En el caso de la Administración de Justicia española, propugnados tanto por el RDL 6/2023, de 19 de diciembre como por la Instrucción 2/2026, de 28 de enero del pleno del CGPJ.