# LA INTELIGENCIA ARTIFICIAL: ¿INNOVACION O AMENAZA PARA LAS GARANTIAS PROCESALES EN LA JUSTICIA PENAL?

## ARTIFICIAL INTELLIGENCE: INNOVATION OR THREAT TO PROCEDURAL GUARANTEES IN CRIMINAL JUSTICE?

CARLA IRENE FURINGO[1]

Doctoranda en Ciencias Jurídicas Universidad Católica (Buenos Aires, Argentina)



[1] Doctoranda en Ciencias Jurídicas Universidad Católica (Buenos Aires, Argentina). Graduada de abogada en la Universidad Nacional de Lomas de Zamora año 2003, especialista en justicia constitucional y crimen organizado por la Universidad de Boloña, profesora adjunta en la Universidad Nacional de Lomas de Zamora, catedra instrumento del derecho Comercial, integrante del proyecto de investigación PICTO 2017-0032 de la Universidad Católica Argentina, integrante del proyecto de investigación del Centro de estudios judiciales de la Universidad Nacional de Lomas de Zamora. Agente fiscal en la provincia de Buenos Aires Argentina, correo carla.furingo@yahoo.com.ar.

**Resumen:** La integración de la inteligencia artificial (IA) en la justicia penal genera tensiones entre la eficiencia judicial y el respeto de los derechos y garantías procesales fundamentales. Si bien la IA puede, sin duda, agilizar los procedimientos, mejorar la administración y proporcionar herramientas predictivas para la toma de decisiones, también plantea serios riesgos debido a posibles sesgos y opacidad algorítmica, donde se puede ver vulnerado el derecho a la tutela judicial efectiva, el derecho de defensa, o la presunción de inocencia. Para garantizar un juicio justo, es esencial la implementación de mecanismos de supervisión humana, transparencia y rendición de cuentas. Un despliegue ético, legal y basado en los derechos humanos es crucial para mantener el equilibrio entre un sistema de justicia penal basado en los derechos y estas nuevas tecnologías.

**Palabras clave**: Inteligencia artificial, justicia penal garantías fundamentales.

**Abstract:** The integration of artificial intelligence (AI) into criminal justice creates tensions between judicial efficiency and respect for fundamental procedural rights and guarantees. While AI can undoubtedly expedite procedures, improve administration, and provide predictive tools for decision-making, it also poses serious risks due to potential biases and algorithmic opacity, which can undermine the right to effective judicial protection, the right to a defense, or the presumption of innocence. To guarantee a fair trial, the implementation of human oversight, transparency, and accountability mechanisms is essential. An ethical, legal, and human rights-based deployment is crucial to maintaining a balance between a rights-based criminal justice system and these technologies.

**Key words**: Artificial intelligence, criminal justice, fundamental guarantees.

## I. INTRODUCCIÓN

La utilización de la inteligencia artificial ha revolucionado el mundo, desempeñando un papel fundamental en el ámbito de la justicia penal, su aplicación no es solo en materia de prevención del delito sino también en la investigación criminal y el proceso judicial.

Las herramientas basadas en IA se han vuelto indispensables para el análisis de datos y la identificación de tendencias delictivas, ofreciendo información que antes era inalcanzable. Estas herramientas pueden analizar enormes volúmenes de datos legales y financieros

para discernir patrones y tendencias, fundamentales para comprender y prevenir actividades delictivas[2]. La capacidad de la IA para procesar y visualizar conjuntos de datos complejos permite detectar rápidamente tendencias emergentes y amenazas potenciales.

Este estudio se propone examinar cuáles son los beneficios como así también los riesgos éticos asociados al uso de la inteligencia artificial en el sistema de justicia penal. Adelantamos nuestra postura que somos partidarios de la aplicación de la innovación y la tecnología en todos los aspectos de la vida cotidiana de los hombres, incluyendo el jurídico. Así también, debemos ser conscientes que su implementación plantea importantes consideraciones y desafíos éticos, en materia de justicia penal, planteando con especial énfasis los problemas derivados de la automatización, la afectación de las garantías constitucionales de del derecho a defensa presunción de inocencia y tutela efectiva.

El objetivo de este trabajo de investigación es contribuir a un debate informando sobre cómo utilizar los potenciales de estas nuevas tecnologías, y al mismo tiempo que su uso garantice la protección de los derechos humanos fundamentales y la integridad del sistema de justicia.

Por lo tanto en primer lugar vamos a analizar el concepto de IA, en segundo lugar, vamos a examinar el impacto de la inteligencia artificial en la justicia penal, estableciendo si fortalece los derechos fundamentales o es una amenaza para las garantías constitucionales, asimismo vamos a estudiar la inteligencia artificial dentro del proceso penal español como prueba electrónica, jurídica y científica, analizando la opacidad algorítmica y estableciendo los niveles de riesgos que existen con su utilización en el proceso penal .-

## II. CONCEPTO DE INTELIGENCIA IA

En la actualidad existen múltiples definiciones de que se entiende por (IA). Los autores Russell & Norvig[3], señalan que la inteligencia artificial es la ciencia que busca crear sistemas que piensen o actúen como los humanos, o piensen o actúen racionalmente. La inteligencia artificial, como inteligencia que puede resolver problemas como la inteligencia humana, se denomina inteligencia artificial general, que se distingue de la inteligencia artificial limitada.

[2] TORRES, M, La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal, Revista Usal, vol. 183 año 2024.

[3] RUSSELL, S. & NORVIG, P., La Inteligencia Artificial, Pearson Prentice Hill, Madrid.2004.

A diferencia de lo señalado anteriormente se advierte coincidencia por parte de la doctrina sobre la llamada teoría triárquica de la inteligencia realizada por el catedrático Robert J. Sternberg[4], que nos ayuda a comprender mejor la IA. Según esta teoría, existen tres tipos de inteligencia: (i) inteligencia analítica o de componentes, la capacidad de adquirir, almacenar, modificar y procesar información; (ii) inteligencia práctica o contextual, que describe la capacidad humana de adaptarse al entorno; y (iii) inteligencia creativa o experiencial, la capacidad de aprender de la experiencia.

En este sentido, es necesario señalar el concepto de inteligencia artificial realizado por la Comisión Europea, que lo define como un sistema informático con la capacidad de hacer tareas sin la intervención humana, por lo que cuando los algoritmos de aprendizaje se están ejecutando, no existe un control humano sobre la combinación y comparación de los datos[5].De igual modo, debemos traer a colación la reciente definición del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio, por el que se establecen normas armonizadas en materia de inteligenciar artificial, en su artículo 3.1): la cual la define como un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales"[6].

## III. ALGORITMOS Y OPACIDAD ALGORÍTMICA

En consecuencia, para hablar de IA, primero debemos examinar los algoritmos como componente fundamental del análisis y la comparación de datos; además, debemos considerar las bases de datos y

[4] Teoría expuesta en Sternberg, R.J. (1985). *Beyond IQ: A Triarchic Theory of Intelligence*. Cambridge: Cambridge University Press.

[5]Comisión Europea (2018). IA para Europa. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. COM (2018) 237 final [SWD (2018) 137 final] Bruselas, 25 de abril de 2018, 1.

[6]Parlamento Europeo (2024). Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se está brecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013,(UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

el big data. Esto nos lleva a los dos pilares principales de la inteligencia artificial: los algoritmos y las bases de datos.

La real academia española define algoritmo como "conjunto ordenado y finito de operaciones que permiten hallar la solución de un problema"[7], es decir, una serie de ecuaciones matemáticas interrelacionadas generan un resultado. Estos algoritmos operan con una gran base de datos, identifican patrones y aprenden de ellos para predecir eventos futuros. Por lo tanto, su desarrollo requiere un proceso lógico-matemático basado en la recopilación, preparación y análisis de datos para obtener resultados fiables.

Los algoritmos se implementan de la siguiente forma:

i) Recopilación y preparación de datos: Esto incluye definir los datos que se recopilarán y el método de recopilación, así como identificar a los responsables de la recopilación de datos y las variables; ii) Desarrollo de algoritmos e implementación de IA: Los algoritmos y la IA se comportan según reglas programadas y, por lo tanto, deben ser útiles, fiables y relevantes para la población; iii) Definición de los protocolos administrativos necesarios para la comercialización del producto: Dado que la IA no necesariamente comprende el contexto simplemente aplicando un algoritmo predefinido, cualquier decisión que afecte a una vida humana debe estar sujeta a supervisión; y iv) Interacción del producto con el marco legal: El acceso público a la información es necesario para la toma de decisiones participativa, lo que requiere el desarrollo de una política de datos abiertos por parte del gobierno.

La inteligencia artificial (IA) nos acompaña desde hace años, operando siempre según los algoritmos descritos. Sin embargo, en los últimos años ha experimentado un cambio de paradigma[8]. Ya no se limita al razonamiento determinista basado en los criterios definidos por un programador para dichos algoritmos. En cambio, se están implementando sistemas de aprendizaje automático que permiten a la IA aprender de sus errores y mejorar de forma autónoma, de manera similar a como los humanos interpretan y razonan. El programador ya no puede analizar el algoritmo ni comprender las decisiones de

[7]ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23. ª ed., [versión 23.7 en línea]. https://dle.rae.es/algoritmo visto el 18/07/2025.

[8]CATERINI, M. (2022). El sistema penal en la encrucijada ante el reto de la inteligencia artificial. Revista de los Estudios de Derecho y Ciencia Política, pág. 35, 4.

la IA[9]. Como veremos más adelante, esto representa una desventaja significativa para su aplicación en procesos penales.

Con el aumento de la complejidad de la IA, el algoritmo depende más de las variables contextuales y las pondera de forma diferente a medida que analiza su significado y los patrones que reconoce. En este punto, los patrones que la IA utilizó para llegar a sus conclusiones se vuelven irreconocibles, lo que pone en entredicho la legitimidad de las decisiones tomadas[10].Aquí se pueden distinguir los diferentes tipos de inteligencia artificial (IA)[11]. Por un lado, están las llamadas IA débiles, que resuelven problemas con variables definidas. Esto incluye también las IA que utilizan algoritmos predefinidos pero carecen de capacidades de aprendizaje automático. Por otro lado, está la IA general. Esta abarca las IA que pueden resolver tareas intelectuales que los humanos con habilidades de razonamiento lógico también pueden realizar y que superan la prueba de Turing. Integran el aprendizaje automático y crean sus propias redes neuronales.

En resumen, la IA se basa en algoritmos predefinidos por el programador. Dependiendo de si se integra o no el aprendizaje automático, se crean sistemas que operan de forma más o menos autónoma y pueden gestionar tareas de mayor o menor complejidad. Mientras que la IA débil repite sistemáticamente lo que se le ha programado y también muestra los errores que encuentra, la IA general es capaz de analizar resultados, visualizar errores y corregirse a sí misma. Se puede decir que aprende de forma independiente; de ahí el término «aprendizaje automático». En este punto, cabe mencionar los conceptos de caja negra y caja blanca.

Se habla de caja negra u opacidad algorítmica cuando se desconocen el contenido y la funcionalidad de un algoritmo, así como su estructura y programación. Por lo tanto, es imposible saber cómo funciona internamente la IA para alcanzar el resultado final. En estos casos, se solicitan datos a la IA, esta los proporciona, pero se desconoce cómo los procesó y comparó, por lo tanto si se utilizan en el proceso penal se estaría violando garantías constitucionales fundamentales

[9]BORGES BLAZQUEZ, R. (2020). Sesgo de la máquina en la toma de decisiones en el proceso penal. IUS ET SCIENTIA, pág. 54-71.

[10]PEREZ ESTRADA, M.J. (2019). Capítulo XI. El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías, en S. Barona Vilar, *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad* (238-239). Tirant Lo Blanch.

[11]MORALES HIGUITA, L.; AGUDELO LONDOÑO , S.; MONTOYA RAIGOSA, M. y MONTOYA VIDALES, A.M. (2021). Inteligencia artificial en el proceso penal: análisis a la luz del Fiscal Watson. *Pensamiento Jurídico*, pág. 54, 147-164.

como el derecho de defensa y la presunción de inocencia, como ya lo hemos plasmado anteriormente[12].

Las cajas negras representan el principal obstáculo para la admisibilidad de la IA como prueba en procesos penales. En contraste, existen las cajas blancas. Se trata de sistemas de IA desarrollados con pleno conocimiento de la estructura interna del algoritmo y del software. En estos casos, el programador comprende el sistema interno, así como su procesamiento y análisis de datos. Esto permite comprender los resultados y las conclusiones del algoritmo. Los sistemas de caja blanca deberían ser obligatorios en todos los sistemas de IA destinados a ser utilizados como prueba en procesos penales, ya que nos permiten supervisar y verificar sus procesos internos.

Todos los sistemas de IA destinados a ser utilizados como prueba en procesos penales deberían estar obligados a utilizar sistemas de caja blanca, ya que estos sistemas nos permiten supervisar y verificar sus procesos internos.

Es innegable que cada vez se desarrollan más sistemas de IA capaces de realizar tareas cada vez más diversas, lo que conlleva su uso generalizado y, por tanto, su presencia en la esfera pública. Esta proliferación, a su vez, también entraña peligros potenciales y la violación de derechos fundamentales mediante el uso de la IA.

En este trabajo solo presentaremos brevemente los sistemas de IA más comunes y utilizados en comisarías y juzgados españoles,[13]conscientes de que esta descripción general quedará obsoleta con el tiempo debido al rápido desarrollo de estas tecnologías.

## IV. INTELIGENCIA ARTIFICIAL Y PROCESO PENAL: ¿HERRAMIENTA DE FORTALECIMIENTO DE DERECHOS FUNDAMENTALES O AMENAZA PARA LAS GARANTÍAS PROCESALES?

La incorporación del sistema de IA en el ámbito jurídico constituye una transformación en la función jurisdiccional. El sistema jurídico, es el instrumento esencial del estado mediante el cual los tribunales

[12]RAMIREZ CARABAJAL, D.M. (2021). El debido proceso de cara a las cajas negras, en D. Guerra Moreno. *Constitución y justicia digital* (185-204). Grupo Editorial Ibáñez.

[13]Para ahondar en detalle sobre más herramientas de IA que se usan en el ámbito policial y judicial véase Cuatrecasas Monforte, C. (2022). La Inteligencia Artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos. [Tesis Doctoral, Universitat Ramon Llull].

resuelven y dirimen los conflictos intersubjetivos y sociales dentro de una comunidad[14], se fundamenta en un conjunto de principios, derechos y garantías a los que las partes tienen derecho para asegurar la igualdad en todo momento. Más específicamente, el procedimiento penal se establece como el medio por el cual se tipifica un delito y se impone una pena; es, por lo tanto, el instrumento del que dispone el Estado para aplicar el derecho penal, en virtud de los principios del Estado de derecho.[15]

La introducción de la IA en el proceso penal no es neutral. El modelo constitucional español de procedimiento penal se caracteriza por su perfil garantista, orientado a la protección de los derechos fundamentales de las personas sometidas a persecución penal. El artículo 24 de la Constitución Española reconoce, entre otras garantías, el derecho a un proceso con todas las garantías, la tutela judicial efectiva, la presunción de inocencia, y los derechos a la defensa y a utilizar los medios de prueba pertinentes para la propia defensa (Constitución Española, 1978). Estas garantías son pilares indispensables del Estado de Derecho y representan obstáculos insuperables para cualquier innovación tecnológica.

En esta orden de ideas, la integración de la IA en los procesos penales representa un verdadero reto para el mantenimiento del estado de derecho[16]. El uso de sistemas de IA como herramienta de apoyo a la administración de justicia, particularmente durante las fases de investigación y juicio, está bien establecido[17]. Dado que su uso será permanente, la búsqueda de eficacia y eficiencia mediante el uso de sistemas de IA, y los beneficios asociados, no deben implicar una vulneración de los derechos humanos fundamentales.

### IV.1. Derecho a tutela judicial efectiva

Dentro de un marco jurídico como la Constitución española, que se caracteriza por su énfasis en garantizar el tratamiento constitucional de los sistemas de protección de derechos y libertades, el derecho a la tutela judicial efectiva reviste especial importancia. Esto

[14]ASENCIO MELLADO, J. M. (2008). *Introducción al Derecho Procesal*. Thomson Reuters Aranzadi.

[15]GOLD SCHMIDT, J. (2021). *Derecho procesal penal y garantías constitucionales*. Editorial Jurídica.

[16]SAN MIGUEL CASO, E. (2023). Justicia penal, inteligencia artificial y control democrático. *Revista de Derecho y Tecnología*, 19(1),pág. 89–115.

[17]DE HOYOS SANCHO, M. (2021). Inteligencia artificial y proceso penal: potencialidades y riesgos. *Revista General de Derecho Procesal*, (54), pág. 1–32.

se debe a que supone, por primera vez, el reconocimiento de una serie de derechos y garantías procesales, cuyo ejercicio se limita a los procedimientos ante los tribunales ordinarios[18]. El derecho a la tutela judicial efectiva es amplio y complejo, e incluye, en resumen, el derecho de acceso a los tribunales, el derecho a una decisión motivada y jurídicamente sólida, el derecho a la efectividad de las resoluciones judiciales y el derecho de apelación[19].

En las últimas décadas, la ineficiencia de la administración judicial se ha hecho cada vez más evidente, reforzando la necesidad de mejorar el derecho a la tutela judicial efectiva y vinculándolo así a la transformación del modelo judicial. En el contexto de la inteligencia artificial (IA), la integración de esta tecnología en el sistema de justicia presenta importantes oportunidades y desafíos para garantizar la preservación y el cumplimiento del derecho a la tutela judicial efectiva y para diseñar sistemas con potencial de mejora en este ámbito. En cualquier caso, debe reconocerse que la eficiencia del sistema de justicia mediante la integración de la IA es fundamental para una cultura de paz[20]. Las aplicaciones de esta herramienta incluyen, en primer lugar, la automatización de procesos burocráticos, lo que facilita la gestión de expedientes, la asignación de casos y la programación de audiencias, evitando así retrasos innecesarios[21]. En segundo lugar, apoya la toma de decisiones mediante el análisis de grandes conjuntos de datos y jurisprudencia relevante, brindando a los profesionales del derecho acceso a más información y permitiéndoles tomar decisiones mejor fundamentadas. En tercer lugar, la IA se utiliza en el ámbito de la resolución alternativa de conflictos, por ejemplo, a través de chatbots de mediación o arbitraje.

Consideramos beneficioso el uso de sistemas predictivos y herramientas inteligentes para apoyar a jueces y fiscales. Sin embargo, sostenemos que, según la Constitución Española y la Ley del Poder Judicial, la administración de justicia y la ejecución de sentencias —es decir, el poder judicial— deben ser ejercidas por jueces humanos, no por sistemas basados en inteligencia artificial. Si bien los sistemas de IA pueden suplir la falta de recursos materiales, humanos y financieros, esto debe hacerse siempre salvaguardando los derechos

[18]RUIZ-RICO, G; CARAZO LIEBANA, M.J. (2013). El derecho de la tutela judicial efectiva. Análisis jurisprudencial, Tirant lo Blanch.

[19]PICO JUNOY, J. (2012), Las garantías constitucionales del proceso, Bosch Editor

[20]FONTESTAD PORTALES, L. (2023). «Eficiencia procesal versus jurisdicción», La Ley Actualidad Civil, 11, pág. 1-12.

[21]NIEVA FENOLL, J. (2016). «La razón de ser de la presunción de inocencia», InDret: Revista para el Análisis del Derecho, 1, pág. 1-23.

y garantías de las partes, como el derecho a la tutela judicial efectiva. Sustituir a un juez por un juez humano contradiría el concepto mismo del poder judicial y el derecho legalmente garantizado a un juez imparcial[22].

El uso de estos mecanismos como herramientas para los jueces no puede ser irrestricto, dados los desafíos éticos y legales que conlleva. El problema del sesgo algorítmico es particularmente relevante: la inteligencia artificial se entrena con una amplia gama de datos históricos, que pueden contener sesgos de índole racial, de género o socioeconómica. Si estos sesgos no se eliminan, podrían generar recomendaciones que perpetúen las desigualdades y, por lo tanto, pongan en peligro la igualdad ante la ley y la imparcialidad judicial. Asimismo, puede haber falta de transparencia y explicabilidad, ya que los algoritmos son complejos y difíciles de comprender para los profesionales del derecho y la ciudadanía, dado que se generan mediante fórmulas matemáticas complejas[23].

La falta de comprensión o la omisión de cuestionar las conclusiones de una IA sin justificación alguna vulneraría el derecho a la tutela judicial efectiva y el derecho a un juicio justo[24] . El apoyo del sistema es una condición, no el único factor decisivo para el juez. En este sentido, alegar indefensión por la falta de explicabilidad de los elementos subyacentes al algoritmo podría equivaler a que el experto no solo justificara su pericia, sino que también revelara cada elemento que lo condujo a ella[25]. Cabe señalar también que la función del juez no se limita únicamente a dictar y ejecutar el veredicto, sino que, como parte de sus deberes, también debe garantizar los derechos y garantías de las partes durante todo el procedimiento, puesto que la decisión final —culpable o no culpable— es el resultado de un largo proceso que difícilmente puede estandarizarse mediante una máquina.

[22]BUENO DE MATA, F. (2020). «Macro datos, Inteligencia Artificial y proceso: luces y sombras», Revista General de Derecho Procesal, 51, pp. 1-31.

[23]La dificultad en las operaciones de su desarrollo puede dar lugar a «cajas negras de datos» en las que el proceso de toma decisiones no sea comprensible. Es esencial que todas las partes comprendan cómo y por qué el algoritmo llegó a tomar esa decisión haciendo así efectivo el derecho a recurrir la decisión tomada.

[24]CANCIO FERNANDEZ, R.C. (2020). ¿Sueñas los jueces con sentencias electrónicas?, *Revista Análisis Jurídico-Político*, (2), 3, pág. 145-168.

[25]CASTELLANOS CLARAMUNT, J; MONTERO CARO, M.D. (2020). «Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales», *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia* (6)2, pág. 72-82.

### IV.2. Presunción de inocencia e Inteligencia artificial

Todo sistema de justicia penal presenta la presunción de inocencia como un elemento clave,[26] porque someter a una persona a un proceso penal como sujeto pasivo conlleva su estigmatización como sospechoso y puede resultar automáticamente en su exclusión social[27]. Su reconocimiento en el artículo 24.2 de la Constitución Española implica que opera como norma de juicio en el proceso,[28] que se aplica en la valoración de la prueba, tanto en lo relativo a la estructura procesal como a la determinación de los hechos. La presunción de inocencia implica, por tanto, que la persona investigada o acusada debe ser tratada como inocente en todo momento, hasta que una sentencia firme y definitiva demuestre lo contrario. Constituye una garantía que debe mantenerse y garantizarse a lo largo de todo el proceso penal y, por consiguiente, en todas sus fases.

Sin embargo, los parámetros del algoritmo de IA pueden incluir evaluaciones que podrían influir en la presunción de inocencia[29], y el uso de esta tecnología no debe imponer restricciones, y mucho menos menoscabar este derecho. Actualmente, existen diversos instrumentos que pueden afectar este derecho. Por ejemplo, existen evaluaciones de riesgo de reincidencia. Los sistemas de IA utilizados para evaluar el riesgo de reincidencia entre los acusados pueden influir en las decisiones relativas a la aplicación de medidas preventivas como la prisión preventiva. Estas evaluaciones suelen basarse en datos históricos que pueden reflejar sesgos geográficos o raciales. En Estados Unidos, por ejemplo, existe el sistema COMPAS (Gestión Correccional de Delincuentes para Sanciones Alternativas), un software que evalúa el riesgo de reincidencia del acusado y asesora al juez sobre el tipo y la duración de la pena aplicable[30]. Pro Publica realizó un estudio so-

[26]La importancia de este derecho se deriva de su reconocimiento en los instrumentos internacionales. Véase en este sentido el art. 11.1 de la Declaración Universal de Derechos Humanos (DUDH) en virtud de cual toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se demuestre su culpabilidad. Así, se recoge de igual modo en el CEDH, en el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) o en el art. 48 dela Carta de los Derechos Fundamentales de la Unión Europea.

[27]NIEVA FENOLL, J. (2016). «La razón de ser de la presunción de inocencia», *InDret: Revista para el Análisis del Derecho*, 1, pág. 1-23.

[28]Véase la STC 128/1995, de 16 de julio, Rec. 993/1995.

[29]SCHUMAN BARRAGAN, G. (2021) «La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE», en S. Pereira Puigvert; F. Ordoñez Ponz (Dirs.), *Investigación y proceso penal en el Siglo XXI. Nuevas tecnologías y protección de datos*, Thomson Reuters Aranzadi, pág. 517-540.

[30]BORGES BLAZQUEZ, R. (2020). «El sesgo de la máquina en la toma de decisiones en el proceso penal», *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia,* (6)2, pp. 54-71.

bre COMPAS que alertó sobre una posible discriminación algorítmica contra las personas afrodescendientes, lo que podría conllevar una violación de la presunción de inocencia[31].Esto demuestra que el uso de la IA en los procesos penales plantea riesgos significativos para la presunción de inocencia, un derecho fundamental dentro del sistema de justicia penal. La naturaleza de la IA y las decisiones basadas en patrones y estadísticas pueden llevar a las autoridades a clasificar erróneamente a individuos como culpables o peligrosos, incluso sin pruebas concluyentes que refuten dicha presunción. Por lo tanto, es esencial que el uso de la IA en el sistema de justicia penal esté sujeto a regulaciones estrictas que garanticen la transparencia y el acceso a la información. Igualmente importante es la inclusión de mecanismos de supervisión humana que permitan la revisión y el análisis de los resultados algorítmicos, salvaguardando así los derechos fundamentales y las garantías procesales del acusado.

### IV.3. El derecho de defensa ante el uso de la inteligencia artificial

En esta orden de ideas, no debemos ignorar el riesgo que el uso de la IA en los procesos penales supone para el derecho a la defensa. Este derecho es un derecho público constitucionalmente consagrado que corresponde a todo acusado, otorgándole la oportunidad de impugnar su sentencia[32]. Esto concierne a un derecho que, junto con la tutela judicial efectiva, es uno de los derechos fundamentales de la ciudadanía y está estrechamente vinculado al Estado de Derecho. Según el proyecto de Ley Orgánica del Derecho a la Defensa[33], que se publicará próximamente tras su aprobación por el Congreso el 30 de octubre de 2024, el derecho a la defensa comprende la asistencia letrada, el acceso a los tribunales, la prevención de dilaciones indebidas y una decisión judicial justa. En particular, en el ámbito penal, incluye el derecho a ser informado de los hechos que se le imputan, el derecho a no declarar contra sí mismo, el derecho a declararse inocente, la presunción de inocencia y el derecho de apelación.

---

[31]ROA AVELLA, M; SANABRIA MOYANO, J.E; DINAS HURTADO, K. (2022). «Uso del algoritmo COMPAS en el proceso penal y los riesgos de los derechos humanos», *Revista Brasileira de Direito ProcessualPenal*, (8)1, pág. 275-310.

[32]ZAFRA ESPINOSA DE LOS MONTEROS, R. (2014). «Sobre el derecho de defensa en la mediación penal», en V.C Guzmán Fluja; I. Flores Prada (Dir.), *Justicia penal y derecho de defensa*, Tirant loBlanch.

[33]Texto disponibleen:https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-6-4.PDF

Al abordar el derecho a la defensa, debemos considerar también el principio de igualdad de armas, que debe respetarse durante todo el proceso para evitar consecuencias adversas o la pérdida de los derechos del acusado. Este debe tener las mismas oportunidades y acceso a los recursos que la parte contraria al presentar pruebas en su defensa [34].La particular importancia de este derecho nos lleva a considerar los riesgos derivados del uso de la IA en los procesos penales. En primer lugar, analizamos la posible dificultad de impugnar las denominadas «pruebas algorítmicas». Con base en el principio de contradicción, entendemos que el uso de algoritmos para recopilar o analizar pruebas en redes sociales, dispositivos técnicos o sistemas de reconocimiento facial puede menoscabar la capacidad de la defensa para impugnarlas. Una configuración defectuosa del algoritmo puede generar falsas alarmas que, sin la debida supervisión humana, pueden perjudicar a las personas. Reiteramos que los sistemas de reconocimiento facial presentan tasas de error significativas, las cuales —al igual que ocurre con los sistemas de vigilancia predictiva— son mayores para ciertos grupos de población. En este sentido, cuando la defensa intenta impugnar una identificación o prueba obtenida mediante IA, puede encontrar importantes obstáculos y limitaciones técnicas que ponen en peligro el principio de igualdad de armas y, por tanto, el derecho a la defensa.

En segundo lugar, y en relación con los puntos mencionados anteriormente, el uso de la IA requiere un profundo conocimiento técnico para cuestionar las pruebas presentadas. En muchos casos, la defensa carece de los recursos necesarios para contratar expertos en análisis técnico. Esto genera un desequilibrio en el proceso, ya que el Estado que dispone de los recursos para utilizar la IA invariablemente tiene un acceso superior a ella. En tercer lugar, la suposición de que los algoritmos son infalibles puede llevar al poder judicial a confiar ciegamente en sus resultados, creando así un sesgo automatizado. Por lo tanto, consideramos que existe un sesgo institucional cuando el resultado de un algoritmo se considera más fiable que las declaraciones de los testigos o del acusado, o posteriormente imputado. Esto conlleva que los argumentos de la defensa pierdan peso frente a los resultados algorítmicos. En cuarto lugar, el reconocimiento y la implementación del acceso a las actuaciones procesales son esenciales en el marco del derecho a la defensa. Este derecho de acceso al expediente del acusado es una de las manifestaciones fundamentales del

[34]RODRIGUEZ BLANCO, A. (2024). «Detectando los riesgos de la Inteligencia Artificial en la instrucción penal», Revista General de Derecho Procesal, 64, pág. 1-66.

derecho a un juicio justo y del derecho a la defensa[35]. Este derecho también incluye la divulgación de los resultados de la investigación y las modificaciones derivadas, así como el derecho a inspeccionar el expediente del caso. Esto último comprende el acceso a todos los materiales, documentos, grabaciones, vídeos y fotografías[36]. Por lo tanto, los elementos obtenidos mediante algoritmos complejos y técnicas de aprendizaje de *deep learning* pueden ser difíciles de interpretar. Si la defensa no puede acceder a los datos y métodos que sustentan una decisión algorítmica, resulta difícil impugnar su validez.

## V. MARCO JURÍDICO DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO DEL PROCESO JUDICIAL ESPAÑOL

Como se mencionó en la sección anterior, actualmente nos encontramos en el apogeo del desarrollo de la IA, incluso en el ámbito jurídico. Por lo tanto, es crucial analizar la importancia de estos métodos de investigación y, en particular, qué tipo de pruebas se pueden obtener mediante herramientas de IA. Dado que se trata de un fenómeno relativamente nuevo y la legislación suele ir a la zaga, no existen regulaciones sobre la IA como prueba. Me atrevería a decir que pasarán años antes de que el Código de Procedimiento Penal incluya una disposición específica sobre esta tecnología. Hasta entonces, no nos queda más remedio que examinar las disposiciones legales vigentes que permiten la IA como prueba, definir los requisitos para su admisibilidad y aclarar cómo deben evaluarla los jueces y tribunales.

En este contexto, algunos juristas han propuesto diversos tipos de pruebas que podrían servir como normas complementarias para las pruebas obtenidas mediante inteligencia artificial. En esta sección, analizaremos si se requiere una redacción específica para regular las pruebas obtenidas mediante esta tecnología, o si, por el contrario, resulta innecesaria conforme a la normativa vigente.

[35]Véase la Circular 3/2018, de 1 de junio, de la Fiscalía General del Estado sobre el derecho de información de los investigados en los procesos penales.

[36]MUERZA ESPARZA, J. (2023). «Algunas cuestiones sobre el derecho de información del investigado», 3, pág. 616-643.

### V.1. La IA como prueba electrónica

La evidencia electrónica se entiende generalmente como «información con valor probatorio que se transmite electrónicamente»[37]. En consecuencia, toda información en medios electrónicos que pueda probar hechos en un procedimiento legal se consideraría evidencia electrónica[38]. Literalmente, esta definición también se aplica a la evidencia obtenida mediante IA, ya que implica información que se genera y se encuentra en medios electrónicos.

Dado que el LECrim no contiene una disposición explícita sobre la prueba electrónica, recurrimos a la Ley de Enjuiciamiento Civil (en adelante LEC) y encontramos en el artículo 299 la disposición que permite "los medios de reproducción de palabras, sonidos e imágenes, así como los instrumentos que permiten el archivo y el conocimiento o la reproducción de palabras, datos, números y operaciones matemáticas realizadas con fines contables u otros fines pertinentes al procedimiento, de conformidad con las disposiciones de esta "Ley", lo que se considera la definición de prueba electrónica.

Más allá del debate conceptual en torno a la prueba electrónica, es prácticamente imposible probar algo exclusivamente por medios electrónicos. Por lo tanto, en los procedimientos judiciales, esta prueba se utiliza como prueba documental, y suele consistir en correos electrónicos, mensajes, grabaciones, fotografías e incluso documentos con firmas digitales. Esta prueba se captura y almacena mediante medios y dispositivos tecnológicos, y se acompaña de un informe de análisis forense informático que confirma su autenticidad.

En consecuencia, la prueba electrónica comprende seis elementos: la autenticidad de la fuente, la integridad e inmutabilidad de la prueba, la inmutabilidad de la prueba desde su forma original hasta su presentación, la trazabilidad que permite el acceso a la fuente original, la posibilidad de recuperar la prueba para su revisión posterior, y su durabilidad y preservación a lo largo del tiempo[39].

En este punto, resulta evidente que la evidencia electrónica se refiere principalmente a aquella que ha existido durante años y que aho-

[37] HERNANDEZ GIMENEZ, M. (2019). Inteligencia artificial y derecho penal. *Actualidad jurídica iberoamericana*, 10, 813.

[38] MUÑOZ RODRIGUEZ, A.B. (2020). El impacto de la Inteligencia Artificial en el Proceso Penal. Anuario de la Facultad de Derecho. Universidad de Extremadura, pág. 695-728.

[39] BUJOSA VADELL, L.M., et al. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), pág. 1347-1384.

ra está en gran medida obsoleta. Sin embargo, los avances tecnológicos han transformado la forma en que se captura y almacena, pasando de lo analógico a lo digital. En otras palabras, hemos reemplazado el correo postal tradicional por correos electrónicos, las fotografías en papel por fotografías digitales y las grabaciones en casete o VHS por grabaciones digitales. Esto ha conllevado un uso más extendido y una mayor huella digital a la que cualquier usuario puede acceder y utilizar como prueba ante un tribunal.

Por lo tanto, el valor probatorio obtenido mediante inteligencia artificial ya no es tan relevante como podría suponerse inicialmente. No obstante, nos proponemos examinar con mayor detalle la cuestión de la prueba electrónica, que se divide en cuatro ámbitos tras la reforma del Código de Procedimiento Penal español (LECrim) de 2015, introducida por la Ley Orgánica 13/2015: la interceptación de comunicaciones telefónicas y electrónicas, la grabación de comunicaciones orales y visuales con dispositivos electrónicos, el uso de dispositivos técnicos para el rastreo, la localización y la captura de imágenes, y el registro de dispositivos de almacenamiento masivo. Además, esto incluye también a agentes cibernéticos encubiertos, rastreadores GPS, el uso de drones y software espía para el control remoto de dispositivos[40].

Llegados a este punto, surge la pregunta de si la normativa vigente sobre pruebas electrónicas puede compensar la falta de regulación de las pruebas obtenidas mediante inteligencia artificial. El término «pruebas electrónicas» puede resultar engañoso y confuso. A primera vista, podría parecer que las pruebas obtenidas mediante IA son un tipo de prueba electrónica, puesto que implican información generada y almacenada por dispositivos electrónicos. Sin embargo, tras un análisis más detallado del concepto y su regulación, las pruebas electrónicas se asemejan más a las pruebas digitales. Esto se debe a que consisten en trasladar los métodos probatorios existentes al ámbito digital, adaptándolos a los avances tecnológicos y reflejando la forma en que se recopilan actualmente dichas pruebas, es decir, las que ya existían. En lugar de generarse de forma analógica y almacenarse físicamente, estas pruebas se generan y almacenan ahora digitalmente gracias a las nuevas tecnologías.

Es cierto que mientras que la evidencia electrónica enfatiza la naturaleza de los datos en sí mismos, siendo estos la fuente de la evidencia, en las herramientas de IA, los datos son lo que el algoritmo

[40] BUENO MATA, F. (2016). Fortalecimiento de garantías procesales y medidas de investigación tecnológica. *Ars Iuris Salmanticensis*, 4, pag 326- 328.

utiliza para generar evidencia. Asimismo en la evidencia electrónica, los datos almacenados en dispositivos electrónicos son la evidencia misma, mientras que en la IA, los datos son la entrada que el algoritmo necesita para generar inferencias que sirven como evidencia. Mientras que en la evidencia electrónica la fuente de la evidencia es la información generada y almacenada en dispositivos electrónicos, en la IA la fuente de la evidencia es la propia IA.

### V.2. La IA como prueba científica

En esta orden de ideas y tras haber examinado la posibilidad de que el marco regulatorio para la evidencia electrónica pueda cerrar la laguna legal en lo que respecta a la evidencia de IA —una posibilidad que personalmente no puedo descartar—, ahora es el momento de evaluar el otro tipo de evidencia que los expertos legales han asociado con la evidencia de IA, a saber, la evidencia científica.

Este análisis es más complejo, ya que no existe una legislación específica que regule la prueba científica. En los procesos penales españoles, dicha prueba se obtiene generalmente mediante peritaje.

Para analizar la prueba científica, debemos comprender dos conceptos: la naturaleza científica de la prueba y la opinión pericial. En primer lugar, la prueba científica requiere una base científica sólida; es decir, el método o la técnica empleados para obtenerla deben ser generalmente aceptados por la comunidad científica. En segundo lugar, requiere la figura del perito que realiza la investigación y la presenta ante el juez o tribunal.

En esta orden de ideas para ser clasificadas como pruebas científicas, las pruebas de IA deben cumplir estos criterios. Por lo tanto, a continuación analizamos hasta qué punto los métodos y técnicas de las pruebas de IA son científicamente sólidos y qué papel desempeña el experto que presenta los resultados y explica los procesos subyacentes.

### V.3. La cientificidad de la prueba por IA

El primer análisis que debemos realizar al considerar la evidencia de IA como evidencia científica es si siquiera puede considerarse ciencia; es decir, aclarar la cuestión de la validez científica de dicha evidencia.

El debate sobre qué constituye ciencia y qué constituye pseudociencia, o qué es ciencia dura y qué es ciencia blanda, puede ser muy interesante, sobre todo porque nuestra legislación no establece un protocolo específico para la admisibilidad de la evidencia científica.

Es aquí donde la llamada validez científica de la evidencia cobra relevancia[41]. Para desarrollar este concepto, debemos remontarnos a 1984, cuando los padres de Jason Daubert presentaron una demanda civil contra Merrell Dow Pharmaceuticals Inc. Este caso llevó a tribunales internacionales a abordar la validez científica de la evidencia utilizada para establecer los hechos: el llamado «caso Daubert»[42].

La demanda presentada por los padres de Daubert contra la compañía farmacéutica fue una de las 1700 reclamaciones que alegaban que uno de sus medicamentos patentados (Bendectin, un antihistamínico utilizado para tratar las náuseas matutinas y los mareos) causaba defectos congénitos en los fetos de mujeres embarazadas cuando se usaba con frecuencia. Ambas partes presentaron dictámenes periciales de sus respectivos especialistas para demostrar la eficacia del medicamento. Debido a la controversia en torno a los diversos estudios presentados por las partes, cuya base científica se consideraba cuestionable, la Corte Suprema de los Estados Unidos desarrolló criterios para evaluar la validez científica de la evidencia[43].

Estos requisitos son:

- La teoría o técnica utilizada debe ser verificable.
- La teoría o técnica utilizada debe haber sido publicada y sometida a revisión por pares.
- La técnica científica utilizada debe especificar un margen de error, así como los estándares de su proceso de desarrollo.
- Estas teorías o técnicas científicas deben gozar de una alta aceptación dentro de la comunidad científica.

Una vez establecida la validez científica de la evidencia, debe evaluarse su calidad y fiabilidad[44]. La calidad de la evidencia depende significativamente de la validez científica de la metodología empleada.

---

[41] VAZQUEZ ROJAS, C. (2014). Sobre la cientificidad de la prueba científica en el proceso judicial. Anuario de Psicología Jurídica, 24, 65-73.

[42] VAZQUEZ ROJAS, C. (2015). De la prueba científica a la prueba pericial. Colección Filosofía y Derecho. Ed. Marcial Pons

[43] Daubert v. Merrell Dow Pharmaceuticals Inc. (509 U.S. 579). 1993.

[44] GASCON ABELLAN, M. (2010). Prueba científica: mitos y paradigmas. Anales de la Cátedra Francisco Suárez, 44, pág. 81-103.

Las pruebas científicas pueden realizarse mediante diversos métodos, pero no todos gozan del mismo grado de aceptación en la comunidad científica. Por lo tanto, es necesario examinar la metodología utilizada para llevar a cabo la prueba científica específica y asegurar que sea la óptima para el caso en cuestión.

Aplicar estos requisitos al campo de la IA implica que una prueba generada por IA solo puede reconocerse como evidencia científica si el algoritmo utilizado cumple con los mismos requisitos. Esto es comprensible, ya que la mayoría de las herramientas de IA utilizadas en análisis forense replican de forma autónoma los métodos y técnicas aplicados por expertos, optimizando así el proceso y haciéndolo más rentable.

En este sentido, la prueba por IA, pueden considerarse evidencia científica si reproducen con precisión la metodología y la técnica subyacentes. Un ejemplo claro es la identificación biométrica mediante IA. Si la IA emplea la misma metodología establecida y generalmente aceptada en la comunidad científica, podemos reconocer la prueba como científica y, por lo tanto, esclarecer la cuestión de su la cientificidad y la calidad de la prueba.

Otro problema, más complejo, es la fiabilidad de esta evidencia. Toda vez que aún no existen regulaciones explícitas que establezcan un protocolo o estandarización, y los desarrolladores de estas herramientas suelen ser empresas privadas, con la excepción de algunas universidades estatales. Cuando se presentan ante un juez o tribunal pruebas científicas, como análisis de ADN o huellas dactilares de un laboratorio oficial, esto se considera un sello de aprobación. El juez no necesita cuestionar la metodología o técnica empleada, el margen de error de los resultados, la calidad del equipo, la formación del perito, etc., ya que se presume que todo está en regla. Esto contribuye a la admisibilidad de la prueba.

En una prueba de IA, el juez debe asegurarse de que se cumplan todos los requisitos pertinentes. Cada organización utiliza su propio algoritmo para operar su IA. Si bien estos se basan en métodos y técnicas científicamente reconocidos, no existe un protocolo estandarizado que garantice la ejecución de dichas pruebas con un algoritmo aprobado por un panel de expertos. Este problema se complica aún más con algoritmos que utilizan cajas negras, como en este caso. Tampoco existe una normativa europea ni nacional que establezca los criterios mínimos que estas instituciones deben cumplir para que su IA reciba el sello de calidad mencionado. Esto, sumado a todo lo anterior, conlleva que los jueces examinen las pruebas generadas por

IA con mayor cautela y con estándares más exigentes; un proceso que las pruebas de ADN ya han experimentado y que ahora también debe afrontar la IA.

### V.4. Cadena de custodia

En cuanto al concepto de cadena de custodia, esta hace referencia a que se garantice que la prueba que ha sido recogida en el lugar del crimen sea la misma que se le muestra al juez en la fase de juicio oral. Para ello existe un registro de cada persona que ha estado en contacto con la prueba, desde el que la recoge hasta el que la presenta en el juicio, pasando por el que la almacena y el que la analiza. En el caso de la prueba por IA no existe una prueba material, pero sí debe registrarse a cada profesional que acceda al software que ejecuta la IA para asegurar que no ha existido ningún tipo de manipulación. A tenor de esto, cerciorarse que los equipos empleados son lo suficientemente seguros frente a cualquier tipo de filtración o hackeo informático.

Por lo tanto, entendemos que las pruebas basadas en IA pueden cumplir con los criterios de rigor científico y fiabilidad, dependiendo del tipo de IA, las técnicas y los métodos empleados los cuales son siempre cruciales. No obstante, cabe señalar que aún queda mucho camino por recorrer para que alcancen el mismo nivel que gozan otro tipo de pruebas científicas, las cuales poseen normas regulatorias y son reconocidas por la comunidad científica.

### V.5. La figura del perito en la prueba por IA:

Los dictámenes periciales son una forma de prueba, elaborada en forma de informe técnico por un experto en una disciplina científica específica, como parte de un procedimiento judicial. Constituyen esencialmente otra forma de prueba, pero se diferencian en que son elaborados por un experto o técnico que asiste al juez o, en su caso, a las partes involucradas. Por consiguiente, el experto es la figura clave. Esto plantea la pregunta: ¿Qué es un experto, quiénes son expertos y quiénes pueden actuar como tales? El experto asiste al juez y compensa su falta de conocimientos especializados en áreas muy específicas. Esta función permite al juez obtener una comprensión integral de los hechos que deben ser evaluados; por lo tanto, los dictámenes periciales y la prueba científica siempre están estrechamente vinculados. Por esta razón, el término «dictamen pericial científico» es más preciso.

Por lo tanto, el término «opinión pericial científica» es más apropiado. Esto se aplica sin excepción a las pruebas de IA, ya que un experto debe explicar las técnicas y los métodos utilizados, especialmente cuando se trata de conceptos abstractos como los algoritmos.

Por consiguiente, es crucial recalcar que la admisibilidad de las pruebas de IA es un requisito indispensable para que la IA opere en un entorno de caja blanca, también conocido como IA explicable. Debemos evitar que se repitan los sucesos del caso Loomis y del caso de IA COMPAS[45], donde se violaron flagrantemente los derechos fundamentales.

Este caso ocurrió en febrero de 2013 tras el arresto y posterior juicio de Eric Loomis, quien fue declarado culpable de robo de vehículo y resistencia al arresto. El caso cobró especial notoriedad cuando su sentencia se determinó mediante una herramienta de evaluación de riesgos basada en inteligencia artificial llamada Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), desarrollada por Northpinte, Inc. COMPAS predice el riesgo de reincidencia de un individuo a partir de un cuestionario de 137 preguntas y sus antecedentes penales.

La defensa de Loomis apeló este veredicto, argumentando que el uso de COMPAS fue inapropiado porque violó su derecho a impugnar la decisión, ya que los criterios y procesos mediante los cuales esta IA calculó y determinó la sentencia no se conocían completamente, puesto que era propiedad privada protegida por derechos de propiedad intelectual; violó su derecho a una sentencia individual, ya que un algoritmo generó datos basados en estadísticas grupales; y, finalmente, su uso constituyó discriminación por motivos de raza y género.

Sorprendentemente, la Corte Suprema de Wisconsin rechazó esta apelación, sentando un peligroso precedente al aceptar el uso de la IA como herramienta de evaluación de riesgos (COMPAS), un precedente que debe evitarse a toda costa en nuestro país. Por lo tanto, es esencial que la IA utilizada en los procedimientos judiciales sea transparente para garantizar que tanto la defensa como el juez comprendan plenamente todos los procesos y métodos que estas tecnologías emplean para llegar a un veredicto. Esto permite el derecho a impugnar los resultados de la IA si se detectan errores, como la consideración de datos sesgados que podrían violar la presunción de inocencia, por ejemplo, al ponderar indebidamente la etnia o el género del acusado.

[45] ROMEO CASABONA, C.M. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *R.E.D.S.*, 13, pag 39- 55.

Basándome en este caso y en el funcionamiento de las evaluaciones de riesgo basadas en IA, considero que nunca deberían admitirse como prueba, ni como opiniones científicas ni como evidencia en general. Estas herramientas no se fundamentan en métodos ni técnicas científicas reconocidas y dependen de bases de datos potencialmente sesgadas. Además, pueden funcionar como una caja negra. Si bien estas herramientas son muy útiles para diversas profesiones, desde policías hasta jueces, esto solo es cierto si basan sus decisiones en su propio criterio y no en predicciones de IA.

Volviendo al tema de los dictámenes periciales: como ya se mencionó en la sección sobre pruebas científicas, estos dictámenes son elaborados por los laboratorios oficiales de las Fuerzas de Seguridad del Estado o el Instituto de Toxicología y Ciencias Forenses del Ministerio de Justicia. Estos laboratorios emiten un informe pericial, que generalmente se adjunta a los demás documentos procesales o probatorios[46]. Es importante destacar los dictámenes elaborados por laboratorios oficiales, ya que poseen un valor probatorio especial y no están sujetos a las normas procesales de los dictámenes periciales ordinarios[47].

Esto se debe a que, como ya hemos mencionado en el caso de la evidencia científica, el ordenamiento jurídico tiene en cuenta la garantía y fiabilidad de los informes técnicos elaborados por laboratorios oficiales, así como la cualificación y experiencia de los peritos que los elaboran. Además, actualmente los laboratorios oficiales realizan análisis de trazas prácticamente instantáneos, lo que permite llegar a conclusiones fiables y difíciles de refutar[48].

Por lo tanto, este tipo de dictamen pericial recibe una consideración especial en comparación con los dictámenes periciales ordinarios, si bien esto no impide que las partes lo impugnen. En tales casos, los peritos que elaboraron el dictamen deben comparecer en la audiencia oral, el dictamen debe leerse en voz alta y, de ser posible, puede ser reproducido o reiterado por otros peritos. En el presente caso, no existen laboratorios públicos comparables que realicen pruebas de IA, razón por la cual este tipo de dictamen no puede recibir esta consideración especial hasta que se produzcan avances en este campo.

[46] PEDRAZ PENALVA, E. (2009). Actividad policial reprochable. Revista de derecho procesal, 1, pág. 763-888.

[47] DOLZ LAGO, M.J., Figueroa Navarro, M.C. y Expósito Márquez, N. (2012). La prueba pericial científica. Ed. Edisofer. Pág. 405 y ss.

[48] BURGOS LADRON DE GUEVARA, J. (1992). El valor probatorio de las diligencias sumariales en el proceso penal español. Ed. Civitas.pag 176-182.

En esta orden de ideas, entendemos que las pruebas basadas en IA pueden cumplir los criterios de los dictámenes periciales, ya que deben ser elaboradas por un experto y confirmadas ante un tribunal. Esto exige que la herramienta utilizada se clasifique como IA explicable, de modo que las partes y el juez puedan comprender todos los procesos llevados a cabo por la IA que condujeron a las conclusiones contenidas en el dictamen pericial correspondiente.

En cuanto la herramienta utilizada opere como caja negra u opacidad algorítmica, esto puede conllevar una violación de los derechos de la persona investigada, como el derecho a impugnar las pruebas o la presunción de inocencia. Por lo tanto, abogamos por la regulación jurídica de las pruebas basadas en IA, no solo para integrarlas en el marco legal, sino también para establecer los criterios necesarios que deben cumplir para prevenir violaciones de los derechos fundamentales.

## VI. NIVELES DE RIESGO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL

### VI.1. Inteligencia predictiva

Estas herramientas de IA sirven para optimizar los recursos y aumentar la eficacia y eficiencia de las medidas de prevención del delito por parte de las fuerzas del orden. Generalmente, estos sistemas de inteligencia artificial analizan datos estadísticos de bases de datos policiales para predecir zonas geográficas con alta probabilidad de actividad delictiva (los llamados puntos críticos) o para identificar a las personas con mayor probabilidad de cometer delitos o ser víctimas. Con esta información, los agentes del orden pueden concentrar su vigilancia en zonas o individuos específicos.

Esta categoría de herramientas de IA se divide en cuatro grupos principales:

1. Herramientas de predicción delictiva: Estas herramientas se utilizan para predecir zonas con alta incidencia delictiva.
2. Herramientas de identificación de delincuentes: Como su nombre indica, estas herramientas crean perfiles de delincuentes para identificar a posibles futuros criminales. Se basan en datos de antecedentes penales y proporcionan descripciones generales.

3. Herramientas de predicción de víctimas: Al igual que el instrumento anterior, este crea perfiles de individuos que podrían ser víctimas de un delito.
4. Herramientas de predicción de delincuentes: Muy similares al instrumento de identificación de delincuentes, pero en lugar de crear un perfil general, generan la probabilidad de que un individuo específico cometa un delito en el futuro.

Mediante estas herramientas, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) toman decisiones estratégicas basadas en pronósticos generales de la actividad delictiva futura, con especial atención al aspecto espacial. Además, se toman decisiones específicas para predecir la presencia de individuos o grupos concretos, así como de delincuentes reales o potenciales. El enfoque en áreas y perfiles específicos permite un despliegue más eficiente de las fuerzas policiales, ya que el objetivo principal es garantizar la prevención más eficaz posible con un número limitado de agentes.

Es importante aclarar que, a pesar del uso de estas herramientas, las decisiones policiales no se basan únicamente en el análisis automatizado de datos personales ni en la creación de perfiles. Se requiere la intervención humana calificada, ya que podría producirse una violación de los derechos fundamentales si un agente de policía detiene a una persona basándose únicamente en la recomendación de una IA. El agente está obligado a considerar siempre todas las circunstancias y tomar la decisión final.[49]

En el contexto de la IA predictiva, cabe mencionar PredPol. Este sistema de vigilancia predictiva es utilizado por departamentos de policía de todo el mundo y se basa en un proyecto de investigación del Departamento de Policía de Los Ángeles (LAPD) y la Universidad de California en Los Ángeles (UCLA). Desarrollada originalmente para predecir el número de bajas en el campo de batalla de Irak, esta IA se ha adaptado para la prevención del delito en el ámbito policial.

Debemos mencionar que en España, COPKIT es uno de los proyectos líderes basados en IA en el ámbito de la predicción y evaluación de riesgos. El proyecto tiene como objetivo desarrollar herramientas de IA para la policía del futuro que respeten los principios de libertad,

[49] Siguiendo esta línea, existe una normativa regulatoria para evitar vulneraciones de derechos tanto a nivel comunitario, con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo; como a nivel estatal con la Ley Orgánica 7/21, 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.

igualdad y justicia. Se centra en analizar, investigar y prevenir el uso indebido de las nuevas tecnologías de la información y la comunicación por parte del crimen organizado y los grupos terroristas.

### VI.2. Inteligencia Artificial de identificación biométrica

Definimos los datos biométricos como datos personales obtenidos mediante procesos técnicos específicos y relativos a las características físicas, fisiológicas o conductuales de una persona que permiten o confirman su identificación unívoca. Esto se corresponde con el artículo artículo 4.14 del Reglamento General de Protección de Datos (RGPD), en el artículo 3.13 de la Directiva sobre protección de datos en el ámbito penal, en el artículo 3.18 del Reglamento (UE) 2018/1725 en la legislación europea y en el artículo 5.1) de la Ley Orgánica 7/2021 en la legislación española.

Por consiguiente, entendemos por herramientas de IA para la identificación biométrica aquellas capaces de identificar a personas concretas mediante la lectura de datos biométricos.

Por lo tanto, existen dos tipos de métodos:

1. Mediciones fisiológicas: Se basan en el análisis de las características físicas y fisiológicas únicas de cada persona, como su rostro, iris o huellas dactilares.
2. Mediciones conductuales: Se basan en el análisis de las características conductuales únicas de cada persona, como su voz, escritura, firma, gestos o estilo de habla y escritura.

Las herramientas de IA que utilizan datos biométricos tienen dos funciones: identificación, es decir, determinar la identidad de una persona desconocida, y verificación, es decir, confirmar que una persona es quien dice ser.

Finalmente, en cuanto a los tipos de herramientas de IA que identifican individuos mediante datos biométricos:

1. Reconocimiento facial: Se basa en la identificación de una persona a través de sus rasgos faciales únicos. Este método es estándar para desbloquear teléfonos inteligentes y para pagos en línea.
2. Reconocimiento de voz: Estas herramientas identifican y verifican a los individuos analizando los sonidos producidos por las vibraciones de las cuerdas vocales y utilizando técnicas de

procesamiento del lenguaje natural (PLN). La voz es una característica tanto fisiológica como conductual y, por lo tanto, varía no solo según la forma y el tamaño de la boca y la garganta, sino también según el acento, los patrones del habla y el vocabulario.

3. Reconocimiento de huellas dactilares: Método para identificar a personas o verificar su identidad mediante el análisis y la comparación de las características de sus huellas dactilares, que son únicas para cada persona.
4. Reconocimiento de firmas y escritura manuscrita: Método para identificar y verificar la identidad de una persona mediante el análisis y la comparación de caracteres y símbolos manuscritos en soportes físicos o digitales.

Este tipo de herramienta resulta sumamente útil en diversos contextos, como la búsqueda de personas desaparecidas, la identificación de delincuentes buscados, el control fronterizo, la identificación de sospechosos en comisarías o juzgados, e incluso la reconstrucción facial y la identificación a partir de declaraciones de testigos. El uso de datos biométricos conlleva riesgos significativos, como la violación de derechos fundamentales y la filtración o el acceso no autorizado a bases de datos.[50]

No obstante, cabe destacar que el uso de datos biométricos, especialmente el reconocimiento facial, plantea inquietudes respecto a la posible violación de derechos fundamentales consagrados en el artículo 18 de la Constitución Española, en particular el derecho a la intimidad personal y a la protección de datos personales, y por consiguiente, la responsabilidad penal por delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio[51].

Para prevenir estas posibles vulneraciones de los derechos humanos y garantías, se sanciono el Reglamento (UE) 2024/1689, en fecha 13 de junio, el cual prohíbe en su artículo 5 el uso de sistemas de identificación biométrica basados en IA para fines generales, a menos que su uso sea necesario para lograr los siguientes objetivos:

[50] Para ahondar en las vulneraciones y riesgos del uso de este tipo de herramientas por IA véase Cuatre casas Monforte, C. (2022). La Inteligencia Artificial en el proceso penal… *op. cit.* nota 24.

[51] JARAMILLO, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital*, 9, pag 20-37.

1. La búsqueda selectiva de víctimas específicas de secuestro, trata de personas o explotación sexual, así como la búsqueda de personas desaparecidas.
2. La prevención de una amenaza concreta, significativa e inminente para la vida o la integridad física de las personas, o de una amenaza real y presente o real y previsible de un atentado terrorista.
3. La investigación o identificación de una persona sospechosa de haber cometido un delito, con el fin de llevar a cabo investigaciones o enjuiciamientos penales, o para ejecutar una sentencia por uno de los delitos enumerados en el Anexo II, que se castiga en el Estado miembro de que se trate con una pena de prisión o una medida de seguridad no superior a cuatro años.

## VII. CONCLUSIÓN

A modo de conclusión, debe reconocerse que, salvo en casos triviales, será imposible maximizar simultáneamente la precisión del instrumento y su absoluta imparcialidad[52]. La realidad no es imparcial. Para evaluarla adecuadamente, debemos aceptarlo. Si queremos que el juez disponga de toda la información necesaria para realizar las evaluaciones más justas y adecuadas, debemos utilizar toda la información posible, incluso la que no esté directamente relacionada con el asunto en cuestión.

Sin embargo, si utilizamos estas herramientas, por ejemplo, para determinar una posible privación de libertad, creo que la información exhaustiva que la IA debería proporcionar al tribunal y permitir al juez centrarse en los aspectos individuales del asunto, incluso considerando toda la información disponible. Por ejemplo, podrían comprender cómo cambia la evaluación de riesgos de la IA si se elimina la condición problemática.

Porque si en un futuro próximo se decide utilizar herramientas basadas en IA para la evaluación de riesgos, como ya ha destacado Slobogin[53], debemos asegurarnos de que cumplan tres requisitos mínimos: idoneidad en cuanto a lo que el juez que toma la decisión realmente necesita saber; validez según parámetros científicos; y equidad.

[52] BERK, R., HEIDARI, H., JABBARI, S., KEARNS, M., y ROTH, A.: «Fairness in Criminal Justice Risk Assessments:…», *ob. cit.* pag. 27.

[53] SLOBOGIN, C. «Principles of Risk Assessment: Sentencing and Policing», end *Ohio St.J. Crim. L.*, vol. 15, 2017, pag. 594 y ss

En mi opinión, esto requiere, como mínimo, que el juez pueda eliminar de toda la información disponible aquellas variables que resulten injustas en la evaluación y evaluar el riesgo de la persona con base en lo que ha hecho o podría hacer.

El uso de cualquier tecnología debe basarse en algo volitivo, no solo en la posibilidad. Debemos incorporar la IA en la justicia penal y la policía, para mejorar la práctica de la justicia penal[54]. Es evidente que no se puede esperar que ninguna IA prediga el futuro. Es obvio, como han dicho Berk y otros, que ninguna herramienta de evaluación de riesgos puede reparar siglos de desigualdad racial o de género[55]. Pero creo que si comprendemos su verdadero alcance, incorporamos una perspectiva ética y legal en un campo dominado por científicos sociales e informáticos, y además tomamos las precauciones necesarias que se derivan del respeto a nuestros derechos y garantías, deberíamos ser capaces de mejorar un poco la justicia gracias a la IA.

## VIII. BIBLIOGRAFÍA


Asencio Mellado, J. M. (2008). Introducción al Derecho Procesal. Thomson Reuters Aranzadi.

Berk, R., Heidari, H., Jabbari, S., Kearns, M., y Roth, A.: «Fairness in Criminal Justice Risk Assessments:…», ob. cit. pp. 27.

Borges Blazquez, R. (2020). Sesgo de la máquina en la toma de decisiones en el proceso penal. IUS ET SCIEN TIA, pag 54-71.

Bueno de Mata, F. (2020). «Macrodatos, Inteligencia Artificial y proceso: luces y sombras», Revista General de Derecho Procesal, 51, pp. 1-31.

Bujosa Vadell, L.M., et al. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. Revista Brasileira de Direito Processual Penal, 7(2), pag 1347-1384.

Burgos Ladron de Guevara, J. (1992). El valor probatorio de las diligencias sumariales en el proceso penal español. Ed. Civitas.pag 176-182.


[54] NIEVA FENOLL, J.: Inteligencia artificial y proceso judicial, editorial Marcial Pons, año 2018.

[55] BERK, R., HEIDARI, H., JABBARI, S., KEARNS, M., y ROTH, A.: «Fairness in Criminal Justice Risk Assessments:…», *ob. cit.* pp. 32 y ss.

Cancio Fernández, R.C. (2020). ¿Sueñas los jueces con sentencias electrónicas?, Revista Análisis Jurídico-Político, (2), 3, pág. 145-168.

Castellanos Claramunt, J; Montero Caro, M.D. (2020). «Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales», IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia (6)2, pág. 72-82.

Caterini, M. (2022). El sistema penal en la encrucijada ante el reto de la inteligencia artificial. Revista de los Estudios de Derecho y Ciencia Política, pág. 35, 4

de Hoyos Sancho, M. (2021). Inteligencia artificial y proceso penal: potencialidades y riesgos. Revista General de Derecho Procesal, (54), pág. 1–32.

Dolz Lago, M.J., Figueroa Navarro, M.C. y Expósito Márquez, N. (2012). La prueba pericial científica. Ed. Edisofer. Pág. 405 y ss.

Fontestad Portales, L. (2023). «Eficiencia procesal versus jurisdicción», La Ley Actualidad Civil, 11, pág. 1-12.

Fuentes Soriano, O. (2016). La intervención de las comunicaciones tecnológicas tras la reforma de 2015. En J. Alonso-Cuevillas Sayrol (Dir.), El nuevo proceso penal tras las reformas de 2015(pp. 261-285). Atelier.

Gardner, H. (1983). Multiple intelligences. Nueva York: Basic Books.

Gascon Abellan, M. (2010). Prueba científica: mitos y paradigmas. Anales de la Cátedra Francisco Suárez, 44, pág. 81-103.

Gold Schmidt, J. (2021). Derecho procesal penal y garantías constitucionales. Editorial Jurídica.

Hern´Andez GimÉnez, M. (2019). Inteligencia artificial y derecho penal. Actualidad jurídica iberoamericana, 10, 813.

Jaramillo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. El Criminalista Digital, 9, pág. 20-37.

Morales Higuita, L.; Agudelo Londoño , S.; Montoya Raigosa, M. y Montoya Vidales, A.M. (2021). Inteligencia artificial en el proceso penal: análisis a la luz del Fiscal Watson. Pensamiento Jurídico, pág. 54, 147-164.

Muñoz Rodríguez, A.B. (2020). El impacto de la Inteligencia Artificial en el Proceso Penal. Anuario de la Facultad de Derecho. Universidad de Extremadura, pág. 695-728.

Muerza Esparza, J. (2023). «Algunas cuestiones sobre el derecho de información del investigado», 3, pág. 616-643

Nieva Fenoll, J. (2016). «La razón de ser de la presunción de inocencia», InDret: Revista para el Análisis del Derecho, 1, pp. 1-23.

Ortiz Padrillo, J. C. (2013). Problemas procesales de la ciberdelincuencia. Colex.

Pérez Estrada, M.J. (2019). Capítulo XI. El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías, en S. Barona Vilar, Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad (238-239). Tirant Lo Blanch.

Richard González, M. (2017). La investigación y prueba de hechos y dispositivos electrónicos. Revista General de Derecho Procesal (43).

Russell, S. & Norvig, P., La Inteligencia Artificial, Pearson Prentice Hill, Madrid.2004.

Pedraz Penalva, E. (2009). Actividad policial reprochable. Revista de derecho procesal, 1, pág. 763-888.

Pico Junoy, J. (2012), Las garantías constitucionales del proceso, Bosch Editor

Roa Avella, M; Sanabria Moyano, J.E; Dinas Hurtado, K. (2022). «Uso del algoritmo COMPAS en el proceso penal y los riesgos de los derechos humanos», Revista Brasileira de Direito Processual-Penal, (8)1, pág. 275-310.

Rodríguez Blanco, A. (2024). «Detectando los riesgos de la Inteligencia Artificial en la instrucción penal», Revista General de Derecho Procesal, 64, pp. 1-66.

Romeo Casabona, C.M. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. R.E.D.S., 13, pág. 39- 55.

Ruiz-Rico, G; Carazo Liebana, M.J. (2013). El derecho de la tutela judicial efectiva. Análisis jurisprudencial, Tirant lo Blanch.

Slobogin, C. «Principles of Risk Assessment: Sentencing and Policing», en Ohio St.J. Crim. L., vol. 15, 2017, pp. 594 y ss

Schuman Barragan, G. (2021) «La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE», en S. Pereira Puigvert; F. Ordoñez Ponz (Dirs.), Investigación y proceso penal en el Siglo XXI. Nuevas tecnologías y protección de datos, Thomson Reuters Aranzadi, pág. 517-540.

San Miguel Caso, E. (2023). Justicia penal, inteligencia artificial y control democrático. Revista de Derecho y Tecnología, 19(1), pág. 89–115.

Torres, M, La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal, Revista Usal, vol. 183 año 2024.

Vazquez Rojas, C. (2014). Sobre la cientificidad de la prueba científica en el proceso judicial. Anuario de Psicología Jurídica, 24, 65-73.

Vazquez Rojas, C. (2015). De la prueba científica a la prueba pericial. Colección Filosofía y Derecho. Ed. Marcial Pons

Zafra Espinosa de los Monteros, R. (2014). «Sobre el derecho de defensa en la mediación penal», en V.C Guzmán Fluja; I. Flores Prada (Dirs), Justicia penal y derecho de defensa, Tirant lo Blanch.