El Criminalista Digital. Papeles de Criminología
II Época, Número 12, 2024, pp. 33-51
ISSN 2340-6046

La inteligencia artificial y su encuadre como medio de prueba
Artificial intelligence and it's frame as a judicial evidence

Enrique Medina Martín[1]

Resumen
La inteligencia artificial es una parte de la ciencia de la computación que, a pesar de existir desde el pasado siglo, está pasando por un desarrollo exponencial que ha ocasionado el surgimiento de innumerables herramientas con posibilidades diversas. Entre estas posibilidades encontramos las llamadas IA predictivas o de evaluación de riesgos e IA de identificación biométrica, cuya incorporación al ámbito de la persecución e investigación criminal supondría grandes ventajas. El problema radica en la falta de regulación propia de este tipo de instrumentos en este ámbito, ya no solo a nivel nacional sino en el plano comunitario; ya que de esto se deriva la posible vulneración de derechos fundamentales y la incertidumbre de los jueces y tribunales a la hora de valorar este tipo de pruebas. Al igual que ocurrió con la irrupción de las tecnologías de las telecomunicaciones o con la prueba de ADN, se requiere que el legislador empiece a construir el lugar que deben ocupar las pruebas por IA, y en este trabajo se pretende analizar si el marco normativo existente puede suplir dicha necesidad mientras se va avanzando en la materia.

Palabras clave
Algoritmo, caja negra, cientificidad, inteligencia artificial, perito, prueba.

Información del artículo:
Fecha de recepción: 11/06/2024
Fecha de aceptación: 25/07/2024

Abstract
Artificial intelligence is a part of computer science that exist since the last century, but nowadays is undergoing exponential development that has caused the emergence of countless tools with diverse possibilities. Among these possibilities we find the so-called predictive or risk assessment AI and biometric identification AI, whose incorporation into the field of criminal prosecution and investigation would entail great advantages. The problem lies in the moment in which this type of tools does not have its own regulation in this area, not only at the national level but at the community level; since this results in the possible violation of fundamental rights and the uncertainty of judges and courts when evaluating this type of evidence. As occurred with the emergence of telecommunications technologies or DNA testing, the legislator is required to begin to build the place that AI testing should occupy, and this work aims to analyze whether the existing regulatory framework can meet this need while progress is made in the matter.

Keywords
Algorithm, artificial intelligence, black box, evidence, proficient, scientificity.

Cómo citar este artículo:
Medina Martín, E. (2024). La inteligencia artificial y su encuadre como medio de prueba, *El Criminalista Digital*, 12, 33-51.

Enlace permanente:
http://revistaseug.ugr.es/index.php/cridi/article/view/31430

[1] Doctor en Criminología.

Sumario: I. Introducción; II. El concepto de inteligencia artificial y su potencial alcance dentro del proceso penal: *1. Definición y bases de la Inteligencia Artificial:* 1.1. Los algoritmos; 1.2. Las bases de datos y la Big Data; *2. Tipos de IA dentro del ámbito de la investigación criminal y el proceso penal:* 2.1. Inteligencias Artificiales predictivas y evaluación de riesgos; 2.2. Inteligencias Artificiales de identificación biométrica; III. El marco jurídico de la inteligencia artificial dentro del proceso penal español: *1. La IA como prueba electrónica; 2. La IA como prueba científica:* 2.1. La cientificidad de la prueba por IA; 2.2. La figura del perito en la prueba por IA; VI. Conclusiones; Bibliografía.

I. Introducción

La Inteligencia Artificial se ha convertido por méritos propios en la nueva tecnología de moda. Mientras hace unos años las empresas dedicadas al sector tecnológico centraban sus departamentos de I+D y sus campañas de marketing en avanzar y destacar los aspectos más relacionados con el *hardware* que con el *software*, como es el caso de los sensores fotográficos en los *smartphone* o de la calidad de los paneles de las televisiones, actualmente las principales mejoras que estas empresas destacan en sus productos son aquellas relacionadas con la IA.

Podemos suponer entonces que la IA es una tecnología que parece dispuesta a irrumpir en la vida de los ciudadanos de las sociedades modernas, y no nos equivocamos al hacerlo. La IA promete ser capaz de liberar a los seres humanos de numerosas funciones, no solo aquellas fácilmente automatizables, además de otorgarnos herramientas que nos permitan realizar tareas para las que no seríamos capaces sin una debida formación previa o sin la ayuda de profesionales.

Y así es, la IA actualmente se encuentra instaurada en empresas para asistir a sus trabajadores en sus puestos de trabajo, e incluso sustituirlos en aquellas funciones que no supongan gran riesgo. También existen herramientas de IA que nos permiten crear ilustraciones, componer melodías o incluso editar vídeos con efectos especiales, sin la necesidad de tener que contratar a expertos especializados o de poseer conocimientos en estas materias.

Y como es de esperar, ya existen herramientas de IA diseñadas para ser utilizadas en el ámbito de la investigación policial y judicial. Llegados a este punto es importante valorar, ya no solo las ventajas y funciones que la IA puede otorgar, sino qué derechos fundamentales pueden verse vulnerados, ya que si por algo se caracteriza el proceso de investigación es por cumplir con todas las garantías.

A raíz de este auge de la IA y de las posibles consecuencias negativas que se pueden derivar de su uso, el Parlamento Europeo ha aprobado recientemente el Reglamento (UE) 2024/1689 conocido como Reglamento de Inteligencia Artificial. Pero a pesar de esta normativa europea, en España no existe un cuerpo normativo que regule aquellas herramientas cuyo funcionamiento se basan en IA y que prometen otorgar pruebas en el seno de una investigación policial.

Esta falta de legislación puede ocasionar que cuando los jueces o tribunales se encuentren ante pruebas obtenidas a raíz de IA, no sepan cómo enfrentarse a ellas. Además, una correcta regulación de las pruebas por IA ayudaría a la estandarización de determinadas herramientas que harían que, tanto el proceso de investigación policial como el proceso penal, se desarrollasen de manera más ágil y fiable.

A falta de esta normativa en materia de la IA como medio de prueba dentro del proceso penal, en el presente texto se analizarán los medios de prueba ya regulados que más puedan asemejarse a la prueba por IA, y si los mismos pueden o no suplir este vacío normativo mientras el legislador avanza en esta materia.

II. El concepto de inteligencia artificial y su potencial alcance dentro del proceso penal

La Inteligencia Artificial (en adelante IA) es un concepto que nos lleva acompañando desde los comienzos de la informática moderna, y es que por entonces el anteriormente mencionado Alan Turing planteó la posibilidad de que

aquellas máquinas capaces de realizar múltiples tareas de forma autónoma pudieran algún día pensar por ellas mismas además de realizar tareas preprogramadas. Fue entonces cuando desarrolló el conocido como Test de Turing[2], una herramienta con el objetivo de analizar la capacidad de una máquina para alcanzar un comportamiento inteligente que se asemeje al del ser humano.

Solemos entender desde esta perspectiva que la Inteligencia Artificial es aquella que le permite a una máquina pensar y actuar igual que un humano, pudiendo incluso llegar a ser consciente de ella misma y alcanzar la conocida como singularidad[3]; y aunque esto suene a un imposible, el mundo de la informática ha avanzado tanto que existen programas que, si no logran alcanzar tal magnitud, si consiguen resultados muy sorprendentes capaz de confundir a cualquier persona no especializada en detectarlas. Y es que actualmente están en auge numerosas IA capaces de imitar voces a la perfección (*FakeYou*[4]), pintar cuadros al mismo estilo que los pintores más famosos *(DeepArt*[5]) o el conocido *ChatGPT*[6] capaz de mantener conversaciones fluidas y utilizado también para realizar escritos, resumir textos e incluso componer canciones.

Este tipo de IA suponen un gran avance no sólo en el ámbito de la informática, sino también ofrece un amplio abanico de posibilidades tanto a profesionales como a la gente de a pie; pero a su vez surgen numerosos inconvenientes que pueden tornarse muy serios como es la suplantación de identidad e incluso incurrir en delitos contra la integridad moral[7]. A pesar de ello, este no es el tipo de IA en el que nos centraremos en este texto, sino en aquellas capaces de otorgar herramientas tanto a las Fuerzas y Cuerpos de Seguridad del Estado (en adelante FCSE) como a los jueces y tribunales, y que, por tanto, puedan servir como medios de prueba.

1. Definición y bases de la Inteligencia Artificial

El concepto de Inteligencia Artificial es difícil de desentrañar en el momento en el que tampoco existe un consenso en torno al concepto de inteligencia. Todos hemos leído u oído acerca de los doce tipos de inteligencia de Howard Gardner[8], pero existe más consenso alrededor de la llamada triárquica de la inteligencia desarrolla por Robert J. Sternberg[9], la cual nos ayudará a comprender mejor en qué consiste la Inteligencia Artificial.

Según esta teoría hay tres tipos de inteligencia: (i) inteligencia analítica o componencial, que se trata de la capacidad de captar, almacenar, modificar y trabajar con la información; (ii) inteligencia práctica o contextual, relacionada con la capacidad de las personas a adaptarse al entorno en el que viven; y (iii) la inteligencia creativa o experiencial, que consiste en la habilidad de aprender a partir de la experiencia.

En cuando al concepto de Inteligencia Artificial, la Comisión Europea que la 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[10]. Por último, debemos

[2] Turing, A.M. (1950). Computing Machinery and Inteligence. *Mind,* 49, 433-460.
[3] Se conoce como singularidad el hipotético momento en el que una Inteligencia Artificial es consciente de sí misma y logra la capacidad de elaborar otros ordenadores o robots que mejoran progresivamente, de forma que cada generación diseñada sería mejor que la anterior llegando a un punto en el que superan al ser humano. Véase Chalmers, D.J. (2010). The singularity: A philosophical análisis. *Journal of Consciousness Studies*, 17, 9-10.
[4] Véase Mordonaba, M. (2024). FakeYou, una inteligencia artificial que imita voces de famosos a la perfección. *20 minutos*. https://www.20minutos.es/tecnologia/inteligencia-artificial/fakeyou-inteligencia-artificial-imita-voces-famosos-5235416/ visto el 18/07/2024.
[5] Véase Polo, D.J. (2023). Así es la inteligencia artificial que pinta cuadros igual que Rembrandt o Van Gogh. *Muy Interesante*. https://www.muyinteresante.com/tecnologia/22980.html visto el 18/07/2024.
[6] Se puede acceder de forma gratuita en https://chatgpt.es/ visto el 18/07/2024.
[7] Es el caso de unos menores investigados en la provincia de Zaragoza por difundir fotografías manipuladas por IA de compañeras de clase. Véase La Vanguardia (2024). Investigados varios menores tras manipular y difundir fotos de compañeras mediante IA. *La Vanguardia*. https://www.lavanguardia.com/vida/20240224/9527549/investigados-menores-manipular-difundir-fotos-companeras-mediante-ia.html visto el 18/07/2024.
[8] Los tipos de inteligencia provienen de la teoría de las inteligencias múltiples de Howard Gardner las cuales se dividen en doce: lingüístico-verbal, lógico-matemática, visual-espacial, musical-auditiva, corporal-kinestésica, interpersonal, intrapersonal, naturalista, emocional, existencial, creativa y colaborativa. Véase Gardner, H. (1983). *Multiple intelligences*. Nueva York: Basic Books.
[9] Teoría expuesta en Sternberg, R.J. (1985). *Beyond IQ: A Triarchic Theory of Intelligence*. Cambridge: Cambridge University Press.
[10] 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.

exponer la definición establecida por el reciente 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):

> "«sistema de IA»: 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"[11].

Se concluye entonces que, para hablar de IA, se hace necesario que nos detengamos previamente en los algoritmos, como parte fundamental en el análisis y comparación de los datos; y también hay que tener en cuenta las bases de datos y la llamada *Big Data*. De esta manera nos encontramos con los dos principales pilares de una Inteligencia Artificial: los algoritmos y las bases de datos.

1.1. Los algoritmos

Según la Academia Española, los algoritmos consisten en un "conjunto ordenado y finito de operaciones que permiten hallar la solución de un problema"[12], una suerte de ecuaciones matemáticas que se van entrelazando para arrojarnos un resultado. Estos algoritmos trabajan en base a un amplio banco de datos, identificando patrones y aprendiendo de ellos para pronosticarlos en un futuro; por lo que para su desarrollo se requiere de un proceso lógico-matemático basado en la recopilación, preparación y análisis de los datos con el objetivo de proporcionar resultados fiables.

Los algoritmos no están programados para afirmar o desmentir una hipótesis planteada, sino que su función es la de correlacionar unos datos con otros mediante un modelo matemático que va analizando datos aleatoriamente hasta que establece un patrón entre ellos, a través del cual podemos realizar apreciaciones con exactitud.

Para lograr esto, los algoritmos se implementan de la siguiente forma:

> "i) recolección de datos y creación: implica la definición de los datos a recolectar y el método para recolectar dicha información, a su vez la definición de quién realizará el mismo y por último el establecimiento de las variables; ii) diseño del algoritmo e implementación de IA: tanto los algoritmos como la IA se comportan en concordancia con las reglas que se han programado, por lo que deben ser útiles, leales e interesar a la población; iii) definir los protocolos administrativos necesarios para sacar el producto: dado que la IA no necesariamente entiende un contexto, aplicando simplemente un algoritmo preestablecido, se hace necesario que toda decisión que afecte una vida humana cuente con supervisión y iv) interacción del producto con el contexto jurídico: si se quiere que las decisiones se tomen de manera participativa, es necesario que las personas puedan acceder a la información, lo que significa construir una política gubernamental de datos abiertos"[13].

Como afirmaba al comienzo, la Inteligencia Artificial lleva años entre nosotros, siempre operando bajo los descritos algoritmos, pero en los últimos años ha sufrido un cambio de paradigma[14], ya que ahora no se limita a deducir de forma determinista bajo los criterios de estos algoritmos predeterminados por un programador, sino que se vienen implementando sistemas de aprendizaje automático, conocido como *machine learning*, que propicia que la IA vaya

[11] Parlamento Europeo (2024). Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen 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).

[12] ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.7 en línea]. https://dle.rae.es/algoritmo visto el 18/07/2024.

[13] Ortiz, J. y Iglesias, C. (2018). Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Angertina and Uruguay. *World Wide Web Fundation*.

[14] Véase 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*, 35, 4.

aprendiendo de sus propios errores y complementándose de forma autónoma de manera similar a la que los humanos podemos interpretar y razonar.

Llegados a este punto, el programador no es capaz de destripar el algoritmo y comprender las decisiones tomadas por la IA[15], lo que supone un gran inconveniente en su aplicación dentro del proceso penal como veremos más adelante. En el momento en el que se introduce el factor *machine learning*, los algoritmos de aprendizaje se van alimentando cada vez de más datos de forma autónoma, volviéndose más complejos y casi imposible de escudriñar.

Conforme la IA va adquiriendo complejidad, el algoritmo va apoyándose en más variables basadas en contexto y comienza a asignar diferentes pesos a cada variable conforme va analizando cuán importante es esa variable y los patrones que percibe. En este punto, no es posible reconocer los patrones que la IA ha realizado para llegar a sus conclusiones, lo que cuestiona la legitimidad de las decisiones que se adoptan[16].

En este punto es donde podemos distinguir los diferentes tipos de Inteligencia Artificial[17]. Por un lado, tenemos la conocidas como IA débiles, que son aquellas que resuelven problemas definidos con variables definidas. En este contexto podemos aunar aquellas IA que hacen uso de algoritmos prestablecidos por un programador pero que no goza de machine learning. En segundo lugar, nos encontramos con la IA general, en las que se aúnan aquellas capaces de resolver tareas intelectuales por cualquier ser humano, incluso capacidad de raciocinio y que son capaces de superar el Test de Turing; y son aquellas en las que se introduce el factor machine learning y que crean sus propias redes neuronales. Por último, tenemos la IA fuerte, que es aquella que es capaz de alcanzar la singularidad y podría tener conciencia de sí misma, realizar procesos cognitivos, aprender, resolver problemas, etc. Sobra decir que estas últimas no existen más allá de películas y videojuegos de ciencia ficción.

En resumen, las IA basan su funcionamiento en los algoritmos, que son preestablecidos previamente por el programador, y que dependiendo de si se les añade o no el factor *machine learning*, nos encontramos con sistemas más o menos autónomos y más o menos capaces de realizar tareas más complejas. Se podría decir que mientras la IA débil repite sistemáticamente para lo que ha sido programada, repitiendo los errores que en su programación se encuentren; la IA general es capaz de analizar los resultados, visualizar los errores y autocorregirse, pudiendo decir que aprende por sí misma y de ahí el concepto de *machine learning*.

Llegados a este punto es necesario mencionar los conceptos de caja negra y caja blanca. Hablamos de caja negra cuando se desconoce el contenido y la función de un algoritmo, cómo fue estructurado y programado, por lo cual, es imposible saber cómo funciona la IA a nivel interno para lograr el resultado final que emite. Son esos casos en los que solicitas unos datos a la IA, esta te los arroja, pero no sabemos cómo ha trabajado con los datos y los ha contrastado[18]. Las cajas negras son el principal escollo para que las IA sean admitidas como medio de prueba dentro del proceso penal, pero de esto hablaremos más adelante.

En el supuesto contrario tenemos el caso de las cajas blancas, donde los sistemas de IA están diseñados bajo el pleno conocimiento de la estructura interna del algoritmo y del *software*. En estos casos el programador conoce el sistema interno y cómo procesa y analiza los datos, por lo que hace posible entender los resultados que el algoritmo nos arroja y sus conclusiones. Las cajas blancas deberán ser exigibles en toda IA que pretenda ser utilizada como medio de prueba en el proceso penal ya que nos permite seguir y verificar sus procesos internos.

Desde el punto de vista del juzgador, las cajas negras son un sistema de entrada y salida. El personal que opera con la IA introduce unos datos y el programa te devuelve un resultado, sin conocer cómo opera internamente y llega a sus conclusiones; por lo tanto, se hace imposible argumentar o contradecir el producto final. Es por esta razón por lo que las

[15] Véase Borges Blázquez, R. (2020). Sesgo de la máquina en la toma de decisiones en el proceso penal. *IUS ET SCIENTIA*, 6(2), 54-71.
[16] Véase 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.
[17] Véase 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*, 54, 147-164.
[18] Véase Ramírez Carvajal, 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.

cajas blancas son condición indiscutible ya que, al conocer el proceso, se puede argumentar o contradecir aquellos pasos que realiza la IA que puedan ser erróneos.

1.2. Las bases de datos y la Big Data

Los algoritmos que forman la estructura de la IA no podrían operar sin unos datos de los que alimentarse. Aunque son los algoritmos los que se llevan el foco y la atención dentro de estas herramientas, debido en parte a su complejidad y el aura de misterio que los envuelve; los datos de los que se alimentan son igual o más importantes que los algoritmos. Unos datos incorrectos o sesgados nos proporcionan Inteligencias Artificiales incorrectas y sesgadas, aunque los algoritmos estén perfectamente programados. Cuanto mayor sea la calidad de los datos que nutran al algoritmo y cuanto mejor, en términos de variables cuantitativas y cualitativas, esté diseñado el código del sistema, menor será el riesgo de estos pronósticos injustos[19]. Es entonces donde entran las bases de datos y la *Big Data*.

Una base de datos no es solamente un almacén físico o electrónico de datos, sino que además estos datos se encuentran sistemáticamente ordenados y conectados entre sí siguiendo una unidad lógica. Dependiendo de los tipos de datos[20], las bases de datos tendrán unas características u otras, pero de forma general las bases de datos son conjuntos de datos estructurados que pertenecen a un mismo contexto para ofrecer un gran cantidad de información. Podríamos decir que una base de datos es una biblioteca, pero en vez de estar compuesta por documentos y textos impresos con un número de copias limitadas, las bases de datos las componen datos y documentos electrónicos ilimitados.

Continuando con el símil, al igual que en una biblioteca los libros se encuentran ordenados en diferentes secciones y mediante unos criterios determinados (fecha, nombre del autor, título del texto, editorial, etc.) para que los usuarios puedan acceder de forma rápida a ellos, en las bases de datos, los datos se encuentran estructurados e interrelacionados según unos criterios determinados por el uso que se hará de ellos. Dependiendo del tipo de base de datos y del tipo de IA, tanto la naturaleza de los datos como su estructuración variará con el objetivo de otorgar resultados rápidos y fiables. Estas bases de datos pueden llegar a alcanzar magnitudes inabarcables para cualquier persona, almacenado millones de *terabytes* de datos que hay que analizar, estructurar y relacionar entre sí, es entonces cuando pasamos al mundo de la *Big Data*.

Los macrodatos, conocidos comúnmente como *Big Data*, hace alusión a conjuntos de datos tan grandes y complejos que se requiere de ingeniería informática para procesarlos y trabajar con ellos. Ahora bien, se hace necesario precisar cuáles son estos datos y de dónde salen, y es que en la sociedad actual hacemos uso exponencial de nuestros dispositivos tecnológicos los cuales consideramos como meros instrumentos, pero que esconden ser grandes generadores de información personal, de modo que dicha información pueda ser recopilada y utilizada para crear inteligencias artificiales con la capacidad de determinar identidades, establecer ubicaciones de sujetos determinados en tiempo real e incluso predecir comportamientos[21].

Y es que, aunque todo esto suene a ciencia ficción, son numerosos, y muy delicados, los datos que otorgamos a las empresas privadas de manera inconsciente. Para desbloquear nuestro *smartphone*, mayoritariamente usamos datos biométricos (reconocimiento de huella o reconocimiento facial) que permiten identificarnos. A su vez, es común tener activado el GPS, instalar aplicaciones bancarias tanto para revisar nuestras cuentas como para hacer pagos o transferencias vía Bizum, realizar compras online en portales de venta como Amazon o Ebay, además de buscar acerca de nuestros intereses en Google. A su vez, aquellos que hagan uso de *smartwatc*h o pulseras digitales generan datos sobre su salud como las pulsaciones por minuto, nivel de oxígeno en sangre e incluso la calidad del sueño. Y no olvidarnos tampoco de toda la información que nosotros mismos publicamos en nuestras redes sociales.

[19] Véase Miró Linares, F. (2018) Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, 20, 87-130.
[20] Para ahondar más en las bases de datos y los tipos de bases de datos y su diseño véase Marqués, M. (2011). Bases de datos. *Ed. Publicacions de la Universitat Jaume I.* Colección Sapientia. 18.
[21] Véase Ortiz Pradillo, J.C. (2022). Inteligencia artificial, Big Data, Tecnovigilancia y Derechos Fundamentales en el Proceso Penal en C. Villegas Delgado y M.ª P. Martín Ríos, *El Derecho de la Encrucijada Tecnológica. Estudios sobre Derechos Fundamentales, nuevas tecnologías e inteligencia artificial*. (103-127). Ed. Tirant lo Blanch.

En conjunto se forma un conglomerado de datos que, de ser bien analizados, estructurados y relacionados entre sí mediante la *Big Data*, se puede extraer información muy delicada que permiten desde determinar nuestros gustos y aficiones -lo que más podría interesar a las empresas a nivel comercial-, hasta identificarnos y geolocalizarnos. Obviamente, en la Unión Europea gozamos de una normativa que nos protege ante el mal uso que las empresas e instituciones públicas puedan hacer con estos datos[22], pero tenemos el caso de China, donde la población hace uso generalizado de dispositivos móviles para multitud de tareas mediante una misma aplicación, WeChat[23], y donde las cámaras de videovigilancia con reconocimiento facial fructifican por toda la ciudad; lo que hace que su población pueda estar controlada por el gobierno. Y es que, como veremos a continuación, las inteligencias artificiales desarrolladas para su uso dentro del ámbito de la investigación criminal van en esa dirección, en la identificación biométrica y en la predicción del comportamiento, entre otras.

2. Tipos de IA dentro del ámbito de la investigación criminal y el proceso penal

Es innegable que el auge las inteligencias artificiales está traspasando los límites de una simple moda pasajera, principalmente porque, aunque sea ahora cuando se habla mucho de ellas, ya llevamos tiempo conviviendo con las mismas. Y es que es innegable que es ahora cuando están surgiendo cada vez más inteligencias artificiales y cada vez son capaces de realizar tareas más diversas, lo que ha propiciado la viralidad de su uso y con ello su exposición al gran público. A su vez, esta proliferación también ocasiona posibles lesiones y vulneraciones a derechos fundamentales propiciadas por el uso de la IA, un aspecto en el que no entraremos a valorar exhaustivamente en el presente texto, pero que origina que estas herramientas sean ajenas al mundo del Derecho.

Cada IA funciona en base a la estructura de sus propios algoritmos y se alimenta de bases de datos de diferentes características, todo ello dependiendo de las tareas para las que hayan sido creadas, en consecuencia, tenemos multitud de tipos de inteligencias artificiales y hacer una clasificación de estas es un trabajo titánico, sobre todo si tenemos en cuenta que cada día surgen nuevas inteligencias artificiales capaces de hacer cosas que ni siquiera podemos imaginar hoy en día. Por esta razón, en este apartado hablaremos solamente, y de manera resumida, de los tipos de herramientas por IA más comunes y de más uso dentro de las comisarías y los tribunales españoles[24], con la seguridad de que quedará obsoleto dentro de un tiempo debido a la expansión de estas tecnologías.

2.1. Inteligencias Artificiales predictivas y evaluación de riesgos

Este tipo de herramientas por IA están dirigidas a optimizar los recursos e incrementar la eficacia y la eficiencias en las tareas de prevención de delitos de las FCSE. De forma general, estas inteligencias artificiales se basan en el análisis de datos estadísticos que se encuentran en las bases de datos policiales con el objetivo de predecir aquellas zonas geográficas donde la posibilidad de que se ejecuten actos delictivos es alta (los conocidos puntos calientes o *hotspots*), o de establecer un perfil personal con mayor probabilidad de cometer delitos o de ser víctima de estos. Con esta información, los agentes policiales concentran la vigilancia sobre determinadas zonas o personas.

Esta categoría de herramientas por IA puede dividirse en los siguientes cuatro grandes grupos:

1. Herramientas de predicción de delitos: aquellas destinadas a pronosticar los puntos calientes o *hotspot* con mayor riesgo de delincuencia.
2. Herramientas de predicción de identidades delictivas: como su propio nombre indica, están diseñada con el objetivo de crear perfiles delictivos para identificar así a posibles delincuentes futuros. Se basan en los datos relacionados a antecedentes penales y arrojan descripciones generales.

[22] El Reglamento (UE) 2016/679 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, la Directiva (UE) 2016/680 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 el Reglamento (UE) 2018/1725 que establece las normas aplicables al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y un Supervisor Europeo de Protección de Datos (SEPD).

[23] WeChat es una aplicación multipropósito china desarrollada por la empresa Tencent, que ofrece multitud de servicios como mensajería instantánea, llamadas telefónicas, redes sociales y pagos *online*.

[24] 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].

3. Herramientas de predicción de víctimas: como la herramienta anterior, pero en esta ocasión se perfilan aquellos individuos con potencial de ser víctimas de un delito.
4. Herramientas de predicción de delincuentes: muy similar al de identidades delictivas, pero en vez de generar un perfil genérico, se enfatiza en la posibilidad de que un determinado individuo delinca en un futuro.

Con estas herramientas, los integrantes de las Fuerzas y Cuerpos de Seguridad del Estado (en adelante FCSE) realizan decisiones estratégicas, basadas en realizar predicciones generales sobre la actividad delictiva futura, con un especial énfasis al plano geoespacial; como decisiones particulares, más enfocadas en predecir sobre individuos o grupos concretos y delincuentes reales o potenciales. El focalizarse en determinadas zonas y determinados perfiles posibilita una mayor economización de los medios policiales, ya que el objetivo final es que, con un número limitado de agentes, la prevención sea lo más efectiva posible.

Se hace necesario puntualizar que, aunque las FCSE hagan uso de estas herramientas, las decisiones de los agentes no se basan únicamente en la automatización de datos personales y elaboración de perfiles, se exige de una intervención humana cualificada ya que podría darse una violación de derechos fundamentales si un agente de policía detiene a una persona determinada simplemente porque lo indica la IA; se exige que el agente siempre tenga que evaluar cada circunstancia y tener la última palabra[25].

Si hablamos de IA predictivas, es de obligada mención la herramienta PredPol, un sistema de vigilancia de naturaleza predictiva que ha sido utiliza en departamentos policiales de todo el mundo y que se basa en un proyecto de investigación entre el Departamento de Policía de Los Ángeles (LAPD) y la Universidad de California-Los Ángeles (UCLA). El origen de esta IA era el de pronosticar víctimas en el campo de batalla de Iraq, la cual se adaptó para predecir el crimen en el ámbito policial.

En España, uno de los proyectos basados en IA a destacar, en materia de predicción y evaluación de riesgos, es COPKIT. Dicho proyecto tiene por objetivo desarrollar herramientas de IA que empleará la policía en un futuro, sin que los mismos vulneren los principios de libertad, igualdad y justicia. Este proyecto se centra en el análisis, investigación y prevención del uso de las nuevas tecnologías de la información y la comunicación por parte del crimen organizado y los grupos terroristas.

Por último, una de las herramienta por IA de evaluación de riesgos más utilizada por parte de la Policía Nacional es el Sistema de Seguimiento Integral en los casos de Violencia de Género (Sistema VioGén). Dicha herramienta se creó con el objetivo de predecir el riesgo de cada individuo implicado en un posible caso de violencia machista, tanto víctima como agresor. Atendiendo a estos riesgos se realizarán o no los determinantes seguimientos y medidas de protección a las víctimas, además de una labor preventiva emitiendo avisos, alertas y alarmas cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima.

2.2. Inteligencias Artificiales de identificación biométrica

Entenderemos por datos biométricos los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de dicha persona, siguiendo de esta forma con lo establecido en el 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 nacional.

Entendemos entonces que las herramientas de IA para la identificación biométrica son aquellas con la capacidad de identificar a personas específicas mediante la lectura de datos biométricos. Estas inteligencias artificiales acceden a

[25] 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.

una base de datos biométricos los cuales comparan con los individuos a analizar para establecer una relación entre ellos e identificarlos. Existen entonces dos tipos de técnicas:

1. Mediciones fisiológicas: aquellas basadas en el análisis de características físicas y fisiológicas únicas de cada persona, como puede ser el rostro, el iris o las huellas dactilares.
2. Mediciones de comportamiento: aquellas basadas en el análisis de características conductuales únicas en cada persona como la voz, la escritura, la firma, la gestualidad o la forma de expresarse oralmente o por escrito.

A su vez, las herramientas de IA que hacen uso de datos biométricos tienen dos funciones: la identificación *per se*, que no es otra cosa que determinar la identidad de una persona desconocida; y la verificación, que es la constatación de que una determinada persona es quien parece o dice ser.

Por último, en cuanto a los tipos de herramientas de IA que identifican haciendo uso de datos biométricos nos encontramos con:

1. Reconocimiento facial: aquellas basadas en reconocer la identidad de una persona mediante la lectura de las características físicas únicas de su rostro. Este método se ha estandarizado para el desbloque de *los smartphones* o para realizar pagos *online*.
2. Reconocimiento por voz: aquellas herramientas que permiten identificar personas y comprobar su identidad tanto por el análisis de los sonidos producidos por la vibración de las cuerdas vocales, como por técnicas de Procesamiento del Lenguaje Natural. La voz es tanto una característica fisiológica como conductual, por lo que no varía solo en función de la forma y tamaño de la boca o la garganta, sino que también del acento, lenguaje y variedad del vocabulario.
3. Reconocimiento de huellas dactilares: aquellas herramientas que permiten identificar a personas o comprobar su identidad mediante el análisis y comparación de los puntos característicos de sus huellas dactilares, que son únicos en cada persona.
4. Reconocimiento de firma y escritura: aquellas herramientas que permiten identificar y verificar la identidad de una persona mediante el análisis y comparación de signos y símbolos manuscritos plasmados en un soporte físico o digital. La firma ha sido el método de verificación por excelencia a lo largo de nuestra historia, pero que a partir del auge de los sistemas informáticos ha ido perdiendo valor.

Este tipo de herramientas son de gran utilidad en diferentes contextos, como en la búsqueda de desaparecidos, identificación de delincuentes en situación de busca y captura, control de fronteras, identificación de sospechosos en sede policial o sede judicial e incluso reconstrucción facial e identificación a través de la descripción de testigos.

El uso de datos biométricos implica grandes riesgos como la vulneración de derechos fundamentales y filtraciones o hackeos de las bases de datos, aspectos que generan una amplia conversación pero que no entraremos a valorar en el presente texto[26]. Aún así, es obligatorio destacar que el uso de datos biométricos, sobre todo del reconocimiento facial, plantea problemas en relación con la eventual conculcación de los derechos fundamentales recogidos en el artículo 18 de la Constitución Española, específicamente a la intimidad personal y la protección de datos de carácter personal, y con ello, la responsabilidad penal por los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio[27].

Para prevenir estas posibles vulneraciones de derechos, el anteriormente mencionado Reglamento (UE) 2024/1689, de 13 de junio, prohíbe en su artículo 5 el uso de los sistemas de IA de identificación biométrica de carácter general, excepto si su uso es necesario para alcanzar los siguientes objetivos:

[26] Para ahondar en las vulneraciones y riesgos del uso de este tipo de herramientas por IA véase Cuatrecasas Monforte, C. (2022). La Inteligencia Artificial en el proceso penal… *op. cit.* nota 24.
[27] Véase Domingo Jaramillo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital*, 9, 20-37.

1. La búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas.
2. La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista.
3. La localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

Trasladándonos a IA de identificación biométricas ya en uso, en el año 2018, por iniciativa del Ministerio de Desarrollo de la Mujer y del Menor de la India, las autoridades policiales crearon una base de datos nacional llamada "*TrackChild*" donde introdujeron miles de fotografías de niños desaparecidos que posteriormente fueron analizadas por una IA de reconocimiento facial de las cámaras de seguridad.

Una de las herramientas más punteras en identificación y reconocimiento facial es la desarrollada por la empresa israelí AnyVision, que es capaz de identificar a una persona en 0,3 segundos a través de las cámaras de seguridad. Este *software* fue adquirido por Mercadona para alertar de aquellas personas que accedían al interior de estos supermercados a pesar de tener una condena o medida cautelar de prohibición de aproximación a cualquiera de los empleados o a los mismos establecimientos.

A raíz de esta decisión, la Agencia Española de Protección de Datos (AEPD) abrió investigaciones al entender que la propuesta de datos basados en el reconocimiento facial con fines identificativos por parte de Mercadona, no estaba autorizada de acuerdo con lo dispuesto por el Reglamento General de Protección de Datos (RGPD).

Ya con anterioridad, la Audiencia Provincial de Barcelona (Sección 9º) se pronunció desfavorablemente en el Auto 72/2021 (Rec. 840/2021), de 15 de febrero, que denegó la autorización a Mercadona para utilizar medios automatizados de captación de datos biométricos para detectar la entrada de condenados a cualquier establecimiento de Cataluña.

Para concluir con este tipo de IA, no todas se centran el en reconocimiento facial e identificación de personas en tiempo real. Existe un proyecto desarrollado entre *Panacea Cooperative Research* y la Universidad de Granada, llamado Skeleton-ID, que es el primer *software* informático de automatización de identificación forense mediante técnicas de antropología física, concretamente de superposición craneofacial.

Esta IA analiza cráneos de restos encontrados, y marca unos determinados puntos característicos correspondientes a la anatomía de la cara. Por otro lado, existe una base de datos con fotografías de personas desaparecidas a las cuales se le realizan el mismo análisis de dichos puntos característicos. Posteriormente, mediante la técnica de superposición craneofacial, se superponen los análisis del cráneo y de las fotografías (tanto de frente como de perfil) en busca de coincidencias.

III. El marco jurídico de la inteligencia artificial dentro del proceso penal español

Como se viene desarrollando en el apartado anterior, estamos viviendo el apogeo del desarrollo de IA, también dentro del plano jurídico, por lo que cabe cuestionarnos dónde encajan esas diligencias de investigación y, más concretamente, los medios de prueba que se hayan obtenido gracias al uso de herramientas por IA.

Debido a que es un fenómeno reciente, y por norma general el Derecho siempre va un paso por detrás, no existe regulación alguna sobre la IA como medio de prueba, y puedo aventurarme a decir que se tardará años en que se contemple y se regule dentro la Ley de Enjuiciamiento Criminal (en adelante LECrim) una mención especial sobre este tipo de tecnologías. Mientras ese momento llega, no queda más remedio que entrar a valorar cuáles son los preceptos actuales que pueden sostener la IA como medio de prueba, cuáles son los requisitos que debe de cumplir para ser aceptados y cómo debe de valorarse por parte del juez o tribunal.

En esta línea, son varios los tipos de medios de prueba propuestos por la doctrina que servirían de regulación supletoria para las pruebas por inteligencia artificial, y en este apartado entraremos a valorar si se requiere de una redacción específica para regular las pruebas derivadas del uso de esta tecnología, o si con los preceptos actuales no se hace necesario.

1. La IA como prueba electrónica

A nivel general, se entiende por prueba electrónica "toda información con valor probatorio incluida o transmitida por un medio electrónico"[28]. Siguiendo esta descripción, cualquier clase de información contenida dentro de medios electrónicos, capaz de acreditar hechos dentro de un proceso, se entenderían como pruebas electrónicas[29]. Tomada esta definición al pie de la letra, dentro de esta podría encajar perfectamente las pruebas obtenidas por IA, ya que es información que se genera y se encuentra dentro de medios electrónicos.

Debido a que no existe una regulación expresa por parte de la LECrim de la prueba electrónica, nos trasladamos a la Ley de Enjuiciamiento Civil (en adelante LEC) para encontrarnos dispuesto en su artículo 299 que "se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevada a cabo con fines contable de otra clase, relevantes para el proceso", considerándose esta la definición de prueba electrónica.

Dejando a un lado la batalla conceptual de la prueba electrónica, a la hora de la verdad es imposible probar de forma electrónica, por lo que este tipo de pruebas se incorporan al proceso como prueba documental, la cual suele consistir en correos electrónicos, mensajes, grabaciones, fotografía, incluso documentos con firma digital; obtenidos y almacenas mediante medios y dispositivos tecnológicos respectivamente, con el consiguiente dictamen pericial informático que asegure la veracidad de los mismos.

Siguiendo esta línea, la prueba electrónica se compone de seis elementos: la autenticidad de la fuente de prueba, la integridad y no alteración de la prueba, la inalterabilidad de la prueba desde su forma original hasta su aportación, la rastreabilidad que permite acceso a la fuente original, la posible recuperabilidad de la prueba a consulta posterior y la perdurabilidad y conservación en el tiempo[30].

Llegados a este punto, vemos que la prueba electrónica hace más referencia a pruebas que nos vienen acompañando desde hace años, y que ya están más que superadas, pero que debido al avance tecnológico el modo en el que se obtienen y se almacenan ha mutado de lo analógico a lo digital. Es decir, hemos cambiado el correo ordinario por el correo electrónico, las fotografías en papel por fotografías digitales o las grabaciones en casete o VHS por grabaciones digitales. Esto ha propiciado tanto la democratización de su uso, como un mayor rastro digital al que todo usuario tiene acceso y que puede incorporar como prueba dentro de un proceso.

En este sentido, la prueba por inteligencia artificial ya no tiene tanta cabida como se podría prever desde un principio, pero sigamos indagando en las cuestiones de la prueba electrónica, ya que tras la reforma de la LECrim en 2015 mediante la Ley Orgánica 13/2015, esta se estructura en cuatro bloques bien diferenciados: la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes, y por último, el registro de dispositivos de almacenamiento masivo de información. Además, se añade la figura del agente encubierto informático, las balizas de GPS, el uso de drones y virus espía para el control a distancia de dispositivos[31].

[28] Hernández Giménez, M. (2019). Inteligencia artificial y derecho penal. *Actualidad jurídica iberoamericana*, 10, 813.
[29] Véase Muñoz Rodríguez, A.B. (2020). El impacto de la Inteligencia Artificial en el Proceso Penal. *Anuario de la Facultad de Derecho. Universidad de Extremadura*, 36, 695-728.
[30] Véase 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), 1347-1384.
[31] Véase Bueno de Mata, F. (2016). Fortalecimiento de garantías procesales y medidas de investigación tecnológica. *Ars Iuris Salmanticensis*, 4, 326-328.

Llegados a este punto es el momento de cuestionarnos si la regulación existente sobre la prueba electrónica puede venir a suplir la falta de regulación de las pruebas obtenidas por inteligencia artificial, y es el que nombre de "prueba electrónica" puede engañarnos y confundirnos. Desde una primera aproximación, la prueba obtenida mediante IA podría pensarse como un tipo de prueba electrónica, ya que es información generada y contenida por dispositivos electrónicos; pero conforme vamos adentrándonos en el concepto y regulación de esta, la prueba electrónica se va tornando más a una prueba digital. Y es que la misma consiste en la traslación de medios de prueba ya existentes al mundo digital, una adaptación al avance tecnológico y a cómo se obtienen esas pruebas en la actualidad, pruebas, repito, que ya existían con anterioridad. En vez de producirse analógicamente y guardarse físicamente, gracias a las nuevas tecnologías, las mismas se producen y almacenan digitalmente.

Cierto es que los datos de los que se sirven las IA pueden ser de la misma índole o que algunas de las tecnologías por IA consisten en una digitalización y automatización de procesos que tradicionalmente se vienen haciendo de forma analógica; pero mientras la prueba electrónica hace énfasis en la naturaleza de los datos, siendo los mismos la fuente de prueba; en las herramientas por IA los datos son de lo que se sirve el algoritmo para proporcionarnos la prueba. Digamos que, en la prueba electrónica, los datos almacenados en dispositivos electrónicos son la prueba *per se*, y en el caso de la IA, los datos son el input que esta necesita para arrojarnos las conclusiones que nos servirían de prueba. Mientras en la prueba electrónica, la fuente de prueba es la información generada y almacenada en dispositivos electrónicos, en el caso de la IA la fuente de prueba es la propia IA.

2. La IA como prueba científica

Una vez explorada la posibilidad de que el marco normativo de la prueba electrónica venga a suplir la carencia legislativa sobre las pruebas por IA, que personalmente considero una posibilidad descartable; es el momento de evaluar el otro tipo de prueba a la que se viene asociando la prueba por IA por parte de la doctrina, que es el caso de la prueba científica.

Este análisis es más complejo que el del apartado anterior ya que no existe una normativa concreta sobre la prueba científica. Cuando este tipo de pruebas sale a la palestra en el proceso penal español, lo hace a través de la figura del perito, en consecuencia, para hablar de prueba científica debemos manejar dos conceptos, la cientificidad de la prueba y la prueba pericial científica.

Y esto es así porque la prueba científica requiere, en primera instancia, de un fundamento científico claro, es decir, que el método o la técnica utilizada para obtener la prueba goce de un consenso dentro de la comunidad científica; y, en segundo lugar, la figura del perito experto, que es el encargado de realizar la prueba y exponerla ante el juez o tribunal.

Dicho esto, para poder englobar a la prueba por IA dentro de la prueba científica debería de cumplir con dichos criterios, por lo que procede a analizar cuánto de ciencia hay en los métodos y técnicas utilizados en las pruebas por IA, y la figura del perito que traslada los resultados y explica los procesos que han dado lugar a los mismos.

2.1. La cientificidad de la prueba por IA

El primer análisis que debemos realizar en el momento en el que planteamos la prueba de IA como prueba científica es si se puede considerar ciencia *per se*, es decir, despejar la incógnita sobre la cientificidad de la prueba por IA.

El debate sobre qué es ciencia y qué es pseudociencia o cuáles son las ciencias duras y las ciencias blandas, puede resultar muy interesante pero también ser demasiado extenso, más aún si tenemos en cuenta que en nuestra legislación no existe ningún protocolo específico para admitir las pruebas científicas.

Es entonces cuando adquiere relevancia la llamada cientificidad de la prueba[32]. Para desarrollar este término es necesario remontarnos al año 1984, cuando los padres del menor Jason Daubert promovieron un juicio civil contra

[32] Véase Vázquez Rojas, C. (2014). Sobre la cientificidad de la prueba científica en el proceso judicial. *Anuario de Psicología Jurídica*, 24, 65-73.

Merrrel Dow Pharmaceuticals Inc., un caso que supuso que los tribunales internacionales se preocuparan por la cientificidad de las pruebas utilizadas para la averiguación de los hechos, el llamado "caso Daubert"[33].

La denuncia de los padres de Daubert contra dicha farmacéutica fue una de las 1700 donde se alegaban que uno de sus fármacos patentados (el Bendectin, un antihistamínico para aliviar las náuseas y mareos propios del embarazo) producía malformaciones congénitas en los fetos de aquellas mujeres embarazadas que lo consumieran con frecuencia. Ambas partes presentaron pericias expuestas por sus propios expertos para probar los efectos de dicho fármaco. Debido a la controversia que generaron los diferentes estudios presentados por las partes por su dudosa base científica, y para ayudar al juez a identificar que una prueba científica y el testimonio del experto pertenezcan al conocimiento científico, la Corte Suprema de los Estados Unidos desarrolló un catálogo de requisitos útiles para constatar la llamada cientificidad de las pruebas[34]. Tales requisitos son:

- La teoría o técnica empleada debe ser comprobada. Lo que distingue a la ciencia es el uso del método científico el cual se basa en la generación y contrastación de hipótesis para comprobar así si pueden ser falsables.
- La teoría o la técnica empleada debe haber sido publicada y ha de encontrarse sujeta a revisión.
- La técnica científica empleada ha de determinar un margen o un porcentaje de error, así también ha de especificar los estándares de su proceso de elaboración.
- Ha de existir un amplio grado de aceptación de estas teorías o técnicas científicas por parte de la comunidad científica.

Una vez constatada la cientificidad de la prueba, habrá que valorar ahora la calidad y la fiabilidad de la prueba científica[35]. En cuanto a la calidad de la prueba, ésta va a depender en gran medida de la validez científica de la metodología empleada. Las pruebas científicas pueden realizarse por diferentes métodos, pero no todos gozan del mismo crédito dentro de la comunidad científica. Es por ello por lo que habrá que tener en cuenta cual es la metodología llevada a cabo para realizar la prueba científica en cuestión y asegurar que es la óptima para ese caso. No obstante, tampoco sobre esto tienen los jueces su parcial conocimiento.

En relación con la fiabilidad, esta también se verá influenciada por la calidad de la técnica empleada, pero esta vez dependiendo de su correcta realización por parte de la entidad que lo realiza. Es fundamental que las mismas posean una infraestructura y personal adecuado, además de que sigan unos rigurosos protocolos a la hora de llevar a cabo los análisis y estudios pertinentes. Pero no solo se hace referencia a la calidad de la técnica empleada por la entidad, sino también al proceso durante el análisis, valorando desde el descubrimiento o registro del indicio hasta su análisis. Por esta razón es muy importante la estandarización de la realización y análisis de las pruebas además de una correcta cadena de custodia.

Para concluir, no debemos de olvidar que las leyes científicas que sirven de base para este tipo de pruebas son mayoritariamente de naturaleza probabilística, por lo que el resultado de una prueba científica es una probabilidad y no una certeza, por muy alta que resulte dicha probabilidad. Es por ello por lo que resulta de vital importancia que el juez o tribunal sepa atribuir a este tipo de pruebas un valor probatorio proporcionado y adecuado, no dejándose llevar por la sobreestimación de la prueba en atención a su carácter científico. La validez de una prueba científica no debe darse por sentada por el hecho de proceder del campo de las ciencias, aunque la misma cumpla con todos los requisitos anteriormente descritos.

Trasladando estos requisitos al ámbito de la IA, entendemos que para que una prueba por IA sea considerada como prueba científica, el algoritmo empleado debe cumplir con los mismos requisitos. Esto no suena muy descabellado ya que la mayorías de herramientas de IA utilizadas en el ámbito forense replican la metodología y técnicas empleadas por los expertos solo que, de manera autónoma, agilizando y economizando el proceso.

[33] Véase Vázquez Rojas, C. (2015). *De la prueba científica a la prueba pericial. Colección Filosofía y Derecho*. Ed. Marcial Pons.
[34] Daubert v. Merrell Dow Pharmaceuticals Inc. (509 U.S. 579). 1993.
[35] Véase Gascón Abellán, M. (2010). Prueba científica: mitos y paradigmas. *Anales de la Cátedra Francisco Suárez*, 44, 81-103.

En ese sentido, la prueba por IA se puede considerar un tipo de prueba científica si replica exactamente la metodología y la técnica en la que se basa. Un ejemplo claro lo tenemos en las pruebas por IA de identificación biométrica, si dicha IA replica la misma metodología que está demostrada y ampliamente admitida por la comunidad científica, entonces podemos admitir dicha prueba como científica, resolviendo así la incógnita de la cientificidad y la calidad de la prueba.

Cuestión diferente, y más compleja, es el tema de la fiabilidad de esta. Trasladémonos al caso de la prueba científica por antonomasia, la prueba de ADN. Para constatar la fiabilidad de la prueba de ADN se requiere, por un lado, que el laboratorio que ha realizado dicha prueba se encuentre homologado, para ello se exige que dicho laboratorio cumpla con una serie de requisitos, como el uso estandarizado de una metodología que se haya demostrado eficiente y que esté totalmente establecida en la comunidad científica, que trabajen con un equipamiento y material que asegure la calidad del proceso y sus resultados, que estén formados por expertos en la materia, y por último que se haya respetado la cadena de custodia; las mismas exigencias que se dan en otro tipo de pruebas científicas como la dactiloscopia, análisis toxicológico, la autopsia, etc. En estos casos, la mayoría de las pruebas las realizan los laboratorios propios de las Fuerzas y Cuerpos de Seguridad del Estado, los Institutos de Medicina Legal y Toxicología estatales o autonómicos, o en su defecto por laboratorios homologados de universidades públicas, todas ellas entidades públicas bajo el paraguas del Estado, presuponiéndose entonces su fiabilidad.

Es aquí donde la prueba por IA se encuentra con dificultades debido a su novedad, y es que todavía no existe una regulación expresa para establecer cualquier tipo de protocolo u homologación, además de que las entidades que realizan este tipo de herramientas suelen ser empresas privadas, exceptuando algunos casos de universidades públicas. Si un juez o tribunal se encuentra ante una prueba científica del tipo ADN o dactiloscopia emitida por un laboratorio oficial, esto supone un sello de calidad que libera al juzgador de plantear cuestiones relacionadas con la metodología o técnica empleada, margen de error de los resultados, calidad de los equipamientos utilizados, formación del experto encargado, etc., presuponiendo entonces que todo ello está en orden, lo que ayuda a la admisibilidad de la prueba.

Sin embargo, ante una prueba por IA el juzgador tiene que cerciorarse de que se cumplen con todos los requisitos pertinentes. Cada entidad emplearía un algoritmo propio para el funcionamiento de su IA, aunque se basen en metodologías y técnicas admitidas por la comunidad científica no existe un protocolo que estandarice este tipo de pruebas y asegure que todas ellas se llevan a cabo mediante un algoritmo aprobado y consensuado por un comité de expertos, asunto que se complica si hablamos de aquellos algoritmos que se sirven de cajas negras, los cuales serían implantables en este caso. Tampoco existe una regulación, ni europea ni nacional, que establezca unos criterios mínimos a seguir por parte de estas entidades para que sus IA gocen de este sello de calidad que mencionamos anteriormente, lo que junto a todo lo anterior propicia que el juzgador encare las pruebas de IA de forma más reticente y con más exigencias, un proceso por el que ya pasó la prueba de ADN y al que se tiene que enfrentar la IA.

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.

Concluimos entonces que la prueba por IA puede cumplir con el criterio de cientificidad y fiabilidad, dependiendo siempre del tipo de IA, las técnicas y los métodos en la que se base. También hay que añadir que aún queda un largo proceso para alcanzar el estándar del que gozan otro tipo de pruebas científicas, ya que poseen consenso dentro de la comunidad científica y regulación normativa.

2.2. La figura del perito en la prueba por IA

La pericia es un tipo de prueba que se practica a través de un informe técnico que un experto de una concreta disciplina científica incorpora al proceso. La pericia no es más que un medio de prueba ordinario, pero con la

particularidad de que es realizada por un experto o técnico que auxilia al Juez, o, en su caso, a las partes, por lo que deducimos que la figura destacada es la del perito. Cabe preguntarse entonces qué es, quién es y quién puede ser el perito.

El perito es un auxiliar del juez que suple su falta de conocimiento en áreas muy especializadas. Es una figura que existe para que el juzgador puede alcanzar un correcto conocimiento de los hechos que enjuicia, de ahí que la prueba pericial y la prueba científica siempre vengan de la mano. Es por ello por lo que lo más correcto es llamarla prueba pericial científica. Esto es totalmente trasladable al caso de la prueba por IA, ya que se requiere de un perito experto que exponga y desarrolle la técnica y los métodos empleados, sobre todo cuanto hablamos de conceptos tan abstractos como los algoritmos.

Es el momento entonces de plantear la necesidad de que, para que una prueba por IA pueda ser admitida, es condición *sine qua non* que la misma funcione a través de caja blanca, conociéndose estas como IA explicables. Se debe evitar que vuelva a darse lo ocurrido en el caso Loomis y la IA COMPAS[36], donde se vulneraron de lleno derechos fundamentales.

Este caso surge en febrero de 2013, tras la detención de Eric Loomis y posterior enjuiciamiento, donde fue declarado culpable por robo de vehículo y eludir a los agentes policiales. Este caso coge especial relevancia en el momento en el que el fallo determinó la duración de la condena a través de una IA de evaluación de riesgos llamada Perfiles de Gestión de Delincuentes Correccionales para Sanciones Alternativa o COMPAS (de las siglas en inglés *Correctional Offender Management Profiling for Alternative Sanctions*) desarrollada por Northpinte, Inc. para predecir el riesgo de incidencia de un individuo a través del análisis de un test de 137 preguntas junto a la información correspondiente a los antecedentes penales.

Este fallo fue recurrido por la defensa de Loomis alegando que el uso de COMPAS es inadecuado ya que se vulnera su derecho de contradicción, ya que no puede conocerse de manera exacta los criterios ni los procesos mediante el cual esta IA calculó y estableció la condena, debido a que la misma era propiedad privada protegida bajo derechos de propiedad intelectual; se vulnera su derecho a una sentencia individualizada, ya que un algoritmo genera datos basados en estadísticas de grupo; y por último su uso constituye una discriminación por razón de raza y género.

Sorprendentemente, el Tribunal Supremo del Estado de Wisconsin rechazó dicha apelación, creando un precedente peligroso al aceptar el uso de una IA como COMPAS, un precedente que se debe evitar en nuestro país. Para ello es indispensable exigir que las IA utilizadas durante un proceso sean explicables, que tanto la defensa como el juez sean conocedores de todos los procesos y métodos utilizados por estas tecnologías para llegar a sus conclusiones. Esto posibilita el derecho de contradicción por si se detecta algún "paso en falso" por parte de la IA, como por ejemplo que se tengan en cuenta datos sesgados que puedan ir contra el derecho de presunción inocencia, como podría ser el caso de preponderar la raza o el género del investigado.

Debido a este caso y al funcionamiento de las IA de evaluación de riesgo, considero que estas nunca deberían admitirse ya no solo como prueba pericial científica, sino tampoco como prueba en general, ya que estas herramientas no se basan ni en métodos o técnicas científicas aceptadas por la comunidad científica y se sirven de bases de datos que pueden estar sesgadas, sin mencionar que pueden funcionar con caja negra. Este tipo de herramientas son de gran utilidad para asistir a los diferentes profesionales, desde agentes policiales hasta jueces, siempre que éstos tomen las decisiones en base a su juicio y no a lo que determine la IA.

Volviendo al caso de las pruebas periciales, y al igual que lo comentado con la prueba científica, la pericia la aportan los laboratorios oficiales de las FCSE o del Instituto de Toxicología y Ciencias Forenses del Ministerio de Justicia, los cuales elaboran un informe pericial en sus laboratorios y que suelen adjuntarse al resto de diligencias o

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

pruebas[37]. Es importante hacer hincapié en las pericias practicadas por laboratorios oficiales, ya que poseen una especial fuerza probatoria y no se les exige una sujeción a las reglas procedimentales de los informes periciales ordinarios[38].

Esto se debe a que, como venimos diciendo con el caso de la prueba científica, el ordenamiento jurídico considera la garantía y la fiabilidad de los informes técnicos emitidos por laboratorios oficiales, junto a la comparecencia y ratificación de los peritos que elaboran dichos informes, además de que en la actualidad los laboratorios oficiales realizan análisis prácticamente inmediatos de vestigios, permitiendo llegar a conclusiones fiables difíciles de impugnar[39].

Por todo ello, este tipo de pericias tienen una consideración especial en relación con la prueba pericial ordinaria, aunque esto no impide que las partes puedan impugnar estos informes, requiriéndose en este caso la comparecencia al juicio oral de los funcionarios periciales que emitieron el informe, la lectura de dicho informe, e incluso, si es posible, se puede reproducir o repetir el informe por parte de otros peritos. Trasladando esto al caso que nos ocupa, no existe nada parecido a esos laboratorios públicos que practiquen pruebas por IA, lo que impide que este tipo de pruebas gocen de esta especial consideración hasta que se avance en esta materia.

A modo de conclusión, afirmamos entonces que la prueba por IA podría encajar dentro de los criterios de la prueba pericial, ya que se requiere de un experto que la realice y la ratifique ante el tribunal. Para ello, es requisito indispensable que la herramienta utilizada entre dentro de las llamadas IA explicables, de manera que las partes y el juez puedan entender todos los procesos que se han llevado a cabo por parte de la IA para llegar a las conclusiones que se incluyen en el pertinente informe pericial.

En el momento que la herramienta utilizada funcione en torno a una caja negra, podría incurrirse en la vulneración de derechos del investigado, como el derecho a contradicción o derecho de presunción de inocencia. Es por ello por lo que desde aquí se demanda la necesidad de la regulación normativa de las pruebas por IA, ya no solo para darles un espacio en el marco normativo, sino para establecer los criterios necesarios que estas deben de cumplir para evitar que se vulneren derechos fundamentales.

IV. Conclusiones

La IA es una tecnología que ha llegado para quedarse debido a las grandes ventajas que aporta a la sociedad, por lo que el Derecho se encuentra en la obligación de regular este tipo de herramientas para evitar que su uso pueda ocasionar cualquier tipo de vulneración de los derechos de los ciudadanos. Además, estas tecnologías se están instaurando en el ámbito de la prevención, persecución e investigación de delitos, lo que refuerza la necesidad de que el legislador trabaje en darle una cobertura lo más pronto posible y asistir así a las FCSE, jueces y tribunales en su uso.

Como se desarrolla a lo largo del texto, el marco normativo de la prueba pericial científica es el que más se ajusta para poder suplir este vacío normativo, siempre y cuando se cumplan determinadas condiciones. En primer lugar, y el requisito más importante, es que la herramienta por IA se base en técnicas y metodologías científicas que gocen de un consenso dentro de la comunidad científica, es decir, que cumpla con los criterios de cientificidad.

Llegados a este punto, no soy partidario de enmarcar aquí las herramienta de IA predictivas y de evaluación de riesgo, ya que su algoritmo no se basa en términos objetivos, sino en valoraciones subjetivas y probabilidades. Lo ideal es que estas herramientas se usen únicamente como asistencia para los agentes policiales a la hora de economizar recursos, como por ejemplo para establecer las rutas de los agentes, focalizarse en puntos conflictivos o estar alerta con determinados perfiles.

Volvamos al ejemplo de COMPAS, una herramienta de IA predictiva y de evaluación de riesgos cuyo funcionamiento no se ajusta a ciencia alguna, sino a un algoritmo programado con datos subjetivos, y podemos afirmar esto ya que uno de los criterios que se tienen en cuenta a la hora de evaluar el riesgo de reincidencia es el de pertenecer a

[37] Véase Pedraz Penalva, E. (2009). Actividad policial reprochable. *Revista de derecho procesal*, 1, 763-888.
[38] Véase Dolz Lago, M.J., Figueroa Navarro, M.C. y Expósito Márquez, N. (2012). *La prueba pericial científica*. Ed. Edisofer. 405 y ss.
[39] Véase Burgos Ladrón de Guevara, J. (1992). *El valor probatorio de las diligencias sumariales en el proceso penal español*. Ed. Civitas. 176-182.

determinada raza o profesar una determinada religión. Esto, además de no ajustarse a ningún criterio científico ni objetivo, vulnera el derecho a la igualdad y el derecho a la presunción de inocencia.

En cuanto a las herramientas de IA de identificación biométrica, serían admisibles siempre y cuando cumplan con el criterio de cientificidad. Por suerte, la mayoría de ellas cumplen con este requisito ya que las herramientas se limitan a replicar las técnicas y métodos de identificación verificadas previamente por la comunidad científica, solo que gracias a la IA el proceso se automatiza. Pero este no es el único punto a valorar, tenemos que hablar también de las cajas negras y cajas blancas. De poco nos serviría una IA de este tipo si no somos capaces de comprender el proceso mediante el cual ha llegado a determinadas conclusiones, lo que le restaría toda credibilidad.

Es por este motivo por lo que es requisito indispensable que para que una prueba de IA sea admitida, además de tener base científica, es que funcione con caja blanca, lo que se conoce en el ámbito como IA explicable. Si volvemos a tomar como ejemplo la IA COMPAS y el caso Loomis, al no tener acceso al código por el cual funciona el *software* desconocemos el proceso mediante el cual la IA llega a sus conclusiones, por lo que el investigado se encuentra ante la imposibilidad de rebatirlos, viéndose así afectado su derecho a contradicción de las pruebas. El juez, para poder valorar la prueba por IA va a requerir que el correspondiente perito sea capaz de exponer los procesos que se llevan a cabo desde que se introducen los datos hasta que se arrojan los resultados, para cerciorarse así de que no se ha producido ningún tipo de error o sesgo a lo largo del proceso.

En conclusión, con el marco normativo actual, la prueba por IA puede ser admitida dentro del proceso penal siempre que cumpla con los mismos requisitos exigidos a la prueba pericial científica. En mi opinión, si la prueba por IA se ajusta a los criterios de cientificidad y es explicable ante el juez o tribunal, es una prueba totalmente válida y que no vulnera los derechos del investigado.

A pesar de ello, se hace necesaria una regulación más explícita para que los jueces y tribunales se encuentren mejor asistidos y puedan valorarla correctamente, ya que aún existen retos por delante en esta materia. Y en esta línea, el próximo paso a seguir es el de la supervisión de los algoritmos que dan estructura y hacen funcionar este tipo de instrumentos.

En España existe la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) con el objetivo de supervisar las IA para que cumplan con la normativa y evitar que vulneren derechos fundamentales, pero esta institución no despeja algunas dudas como la necesidad de que el algoritmo de una IA tenga que ser de dominio público para que pueda ser utilizada como prueba o, si por el contrario, al cumplir con los requisitos marcados por esta institución y una revisión del algoritmo por parte de la misma, son requisitos suficientes para que una herramienta de IA obtenga ese sello de calidad de cara a un proceso judicial penal.

Si trasladamos el debate a una prueba de carácter científico totalmente instaurada como el ADN, cuya regulación normativa también pasó por un proceso similar, el tribunal no exige conocer con exactitud todos los componentes y las licencias necesarias para realizar este tipo de pruebas, las cuales están protegidas por el derecho a la propiedad industrial, sino que es suficiente con demostrar su cientificidad y fiabilidad. Misma situación se puede a trasladar a las pruebas por IA, si las mismas cumplen con dichos criterios, y los algoritmos han sido revisados y aprobados por las instituciones competentes, no sería necesario que estos algoritmo ni las bases de datos fueran de carácter público.

Aun así, este es un debate que no se puede solventar hasta que el legislador apruebe las normas pertinentes en esta materia. Y a pesar de ello, el mundo de la IA evoluciona tan rápidamente que irán surgiendo nuevos escollos que afrontar que hoy día desconocemos o nos parecen inalcanzables, como la automatización de estas IA o incluso que procesos que normalmente se lleven a cabo por humanos, en un futuro se encuentren gestionados por una IA.

Se hace muy difícil plantear una legislación a futuro, y más cuando observamos que al mundo del Derecho le cuesta seguir el ritmo a los avances tecnológicos, pero sí sería inteligente aprovechar la ocasión para, ya no solo legislar sobre las herramientas que están surgiendo en la actualidad, sino también para acotar el camino que queremos seguir dentro del mundo de la Inteligencia Artificial, evitando así problemas futuros.

Bibliografía

BORGES BLÁZQUEZ, R. (2020). Sesgo de la máquina en la toma de decisiones en el proceso penal. *IUS ET SCIENTIA*, 6(2), 54-71.

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

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), 1347-1384.

BURGOS LADRÓN DE GUEVARA, J. (1992). *El valor probatorio de las diligencias sumariales en el proceso penal español*. Ed. Civitas. 176-182.

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*, 35, 4.

CHALMERS, D.J. (2010). The singularity: A philosophical análisis. *Journal of Consciousness Studies*, 17, 9-10.

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

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

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

GASCÓN ABELLÁN, M. (2010). Prueba científica: mitos y paradigmas. *Anales de la Cátedra Francisco Suárez*, 44, 81-103.

HERNÁNDEZ GIMÉNEZ, M. (2019). Inteligencia artificial y derecho penal. *Actualidad jurídica iberoamericana*, 10, 813.

MARQUÉS, M. (2011). Bases de datos. *Ed. Publicacions de la Universitat Jaume I.* Colección Sapientia. 18.

MIRÓ LINARES, F. (2018) Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, 20, 87-130.

MONFORTE, C. (2022). *La Inteligencia Artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos*. [Tesis Doctoral, Universitat Ramon Llull].

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*, 54, 147-164.

MORDONABA, M. (2024). FakeYou, una inteligencia artificial que imita voces de famosos a la perfección. *20 minutos*. https://www.20minutos.es/tecnologia/inteligencia-artificial/fakeyou-inteligencia-artificial-imita-voces-famosos-5235416/

MUÑOZ RODRÍGUEZ, A.B. (2020). El impacto de la Inteligencia Artificial en el Proceso Penal. *Anuario de la Facultad de Derecho. Universidad de Extremadura*, 36, 695-728.

ORTIZ PRADILLO, J.C. (2022). Inteligencia artificial, Big Data, Tecnovigilancia y Derechos Fundamentales en el Proceso Penal en C. Villegas Delgado y M.ª P. Martín Ríos, *El Derecho de la Encrucijada Tecnológica.*

Estudios sobre Derechos Fundamentales, nuevas tecnologías e inteligencia artificial. (103-127). Ed. Tirant lo Blanch.

ORTIZ, J. y IGLESIAS, C. (2018). Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Angertina and Uruguay. *World Wide Web Fundation*.

PEDRAZ PENALVA, E. (2009). Actividad policial reprochable. *Revista de derecho procesal*, 1, 763-888.

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.

POLO, D.J. (2023). Así es la inteligencia artificial que pinta cuadros igual que Rembrandt o Van Gogh. *Muy Interesante*. https://www.muyinteresante.com/tecnologia/22980.html

RAMÍREZ CARVAJAL, 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.

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

STERNBERG, R.J. (1985). *Beyond IQ: A Triarchic Theory of Intelligence*. Cambridge: Cambridge University Press.

TURING, A.M. (1950). Computing Machinery and Inteligence. *Mind,* 49, 433-460.

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

VÁZQUEZ ROJAS, C. (2015). *De la prueba científica a la prueba pericial. Colección Filosofía y Derecho*. Ed. Marcial Pons.