

Derecho de la neurología: Libro blanco para el desarrollo de la
Carta de Derechos Digitales en el ámbito de la neurotecnología
Beatriz Gregoraci, Jorge Castillo Abella y Francisco Velasco Caballero (dirs.)
ISBN: 979-13-87913-93-3
Madrid, 2026
pp. 823-846
DOI: 10.37417/derecho-de-la-neurotecnologia/21
Marcial Pons Ediciones Jurídicas y Sociales
Editado bajo licencia Creative Commons Attribution 4.0 International License

CAPÍTULO XXI

ALGORITMOS E INTELIGENCIA ARTIFICIAL EN LA JUSTICIA PENAL: ¿QUÉ, DÓNDE, CUÁNDO Y CÓMO?

Fernando MARTÍN DIZ
Universidad de Salamanca
fmdiz@usal.es

1. INTRODUCCIÓN: INTELIGENCIA ARTIFICIAL, UNA REALIDAD EN EL ÁMBITO PROCESAL

El primer cuarto del siglo XXI ha deparado, haciendo una recapitulación de sus mayores avances y logros, el asentamiento de la IA como solución tecnológica vanguardista que se expande, prácticamente, a todos los ámbitos de la sociedad, la actividad profesional, científica, económica, educativa o cultural. El mundo jurídico no ha sido, ni va a ser, excepción. Pudiendo parecer lejanas en el tiempo, y excesivamente futuristas, las previsiones de Isaac Asimov en su obra *Yo, Robot*, publicada en 1950, posiblemente, hoy en día, se hayan visto superadas desde los planteamientos de esa colección de relatos que se sustentaba sobre las denominadas «tres leyes de la robótica»¹, como una especie de advertencia moral aplicable a futuros robots «inteligentes», y que

¹ «1. Un robot no puede hacer daño a un ser humano o, por su inacción, permitir que un ser humano sufra daño. 2. Un robot debe obedecer las órdenes dadas por los seres humanos, excepto si estas órdenes entran en conflicto con la Primera Ley. 3. Un robot debe proteger la

no depararían conflictos con los humanos. Hoy, afrontamos cara a cara un mundo digital y tecnológico en que el ser humano, paulatinamente, se puede ir viendo relegado por las máquinas, por las inteligencias artificiales que ya son capaces de hacer casi todo, también impartir justicia y resolver litigios. En definitiva, una realidad incontestable a nivel global y a nivel particular en cuanto afecta al derecho y, especialmente, al derecho procesal. Un avance tecnológico de tal calibre que puede llevarnos, incluso, a la figura y posibilidad del juez-robot, como solución de IA no humana capaz de resolver litigios y de evacuar decisiones o resoluciones que decidan una cuestión jurídica.

No siendo descartable ninguna posibilidad, tampoco la de un juez-robot como máxima expresión de la aplicación de la IA en el ámbito de la justicia, puede ser mucho más provechoso, al menos en este momento, delimitar los contornos claros y concisos en los cuales se pueda utilizar de manera óptima y garantista esta tecnología disruptiva, sin olvidar sus contornos éticos. En este sentido, en relación con esta última variante, es de obligada referencia acudir a las reflexiones de Cortina Orts, quien recuerda en su doctrina cómo los avances técnicos se han anticipado a las orientaciones morales sobre su uso, sin que la IA sea una excepción a esta circunstancia. Considera la autora que, en el estado actual de las cosas, más que plantearse una ética de los sistemas inteligentes puede ser más útil establecer una serie de orientaciones éticas para el uso humano de los sistemas de IA. Aseveración con la que concordamos plenamente, más aún cuando la IA es una creación humana, que demanda siempre el componente humano, no solo en su producción, sino en su posterior supervisión y control. Baste recordar que uno de los principios fundamentales, que han señalado las distintas normas europeas para un uso ético de la IA, ha sido, constantemente, el principio «human in command», que asimila esa idea del control por humano en relación con la actividad desplegada por esta creación tecnológica.

En la amalgama de orientaciones éticas para un uso humano de los sistemas de inteligencia artificial, identifica Cortina Orts las relativas a la confiabilidad y explicabilidad de estos sistemas, su beneficencia —entendida como la exigencia de maximizar los beneficios de su utilización— y no maleficencia —evitando efectos adversos y no previstos— así como el respeto a la autonomía de las personas y la justicia. Todas ellas, por tanto, perfectamente aplicables a la idea de eficiencia que concilie con garantías en la aplicación de la IA en el ámbito de la justicia.

existencia en su misma medida para no autodestruirse en la medida en que esta protección no entre en conflicto con la Primera o la Segunda Ley».

En todo caso, el análisis de las condiciones que puede comportar una utilización garantista de la IA en las actuaciones procesales es compatible con las prevenciones éticas generales de utilización de la misma, basadas en el impacto general que este cambio tecnológico disruptivo determina en la sociedad y sus individuos, así como las transformaciones que a todos los niveles comporta. Desde la UNESCO se plantea, atinadamente, cómo la ética supone una base dinámica para la evaluación normativa y la orientación de las tecnologías de la inteligencia artificial refiriéndose a la dignidad humana, el bienestar y la prevención de daños como «brújula». A partir de estas premisas generales, y como creación humana que es, pasa a ser un acto de responsabilidad individual de quienes la diseñan e implementan el hecho de autoimponerse límites, ante la ausencia de marcos normativos de referencia, salvo en el entorno europeo y gracias a la promulgación y entrada en vigor del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Asumen, por tanto, los creadores de estas herramientas, la responsabilidad de preservar los derechos fundamentales y las garantías procesales que en el ámbito de la justicia son esenciales, y constitucionales, de cara a la utilización de IA, compromiso que se traslada, posteriormente, en su utilización y aplicación en actuaciones procesales a quienes sean los usuarios de dicha herramienta, valorando en ese momento y situación procesal el impacto que su utilización conlleve sin olvidar, como se ha advertido reiteradamente, que la tecnología no es neutral y que debe hacerse siempre desde la fijación y observancia de principios que ofrezcan seguridad y confiabilidad tanto jurídica como general.

Como conclusión a este apartado introductorio, consideramos de interés dos cuestiones. En primer lugar, aportar una definición de qué podemos considerar IA. En segundo lugar, fijar posición, de forma clara e inequívoca, en relación con el desempeño que la IA puede ostentar en el ámbito del proceso judicial.

En relación con la primera cuestión, abordamos seguidamente el envite de ofrecer un concepto de IA. Para ello, tomamos una doble referencia. Inicialmente, la que fue ofrecida en el documento «Directrices éticas para una inteligencia artificial fiable» (Unión Europea, 2018) señalando que se trata de sistemas de *software* (y posiblemente también *hardware*) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital al percibir su entorno a través de la adquisición de datos, interpretando los datos recopilados o no estructurados, razonando sobre el conocimiento, o el procesamiento de la información, derivado de estos datos y la decisión de las mejores acciones a tomar para lograr el objetivo dado. Puede completarse con el concepto más actual y reciente que ofrece el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el

que se establecen normas armonizadas en materia de inteligencia artificial² (RIA) entendiendo que la IA, según dispone el art. 3.1 del RIA, que califica a un sistema de inteligencia artificial 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».

Una IA es, por tanto, una creación humana que, partiendo de unos datos previamente incorporados y procesados mediante unas reglas de tratamiento —algoritmos— introducidas por sus creadores, ofrece un resultado. No perdamos de vista, entonces, la importancia que adquiere su elemento inicial y originario: los datos. Una IA es siempre una creación humana, tecnológica, capaz de evolucionar desde la programación con la que los ingenieros informáticos la diseñan, pero que necesita, como acabamos de señalar, un punto de partida: datos, precedentes, y con ellos saber y conocer situaciones previas, cómo se gestaron, desarrollaron y concluyeron, son, por tanto, absolutamente imprescindibles. La IA y el *big data* están permitiendo el almacenamiento y gestión de millones de datos que, sobre la base de lo acontecido (fenómenos, hechos o antecedentes ya sucedidos), pueden ofrecer conclusiones desde las variables (algoritmos) que los relacionan y procesan. El problema al que debemos enfrentarnos, con carácter previo a la utilización de una IA en el ámbito procesal, viene dado por la concurrencia de datos públicos, datos privados (para los cuales es imprescindible la autorización judicial para ser recabados al amparo del art. 18 CE con la cobertura legal de la LO 13/2015 en relación con las medidas de investigación tecnológica) y datos semiprivados (fundamentalmente los procedentes de redes sociales en los cuales el usuario ha delimitado un restringido grupo de personas que pueden acceder a ellos), determinando en función de su naturaleza cuándo, cuáles y cómo son utilizables a fines de investigación y enjuiciamiento de delitos.

¿Qué debemos entender por datos? La respuesta más concreta la podemos encontrar en el concepto de dato personal que aporta el art. 4.1 del Reglamento UE General de Protección de Datos catalogándolos como «toda información sobre una persona física identificada o identificable (“el interesado”); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisioló-

² Publicado en el Diario Oficial de la Unión Europea de 12 de julio de 2024.

gica, genética, psíquica, económica, cultural o social de dicha persona». Los datos que se incorporan a la configuración y arquitectura de una IA legal deben tener una procedencia lícita, fiable, actual y actualizada, no manipulada, ni sesgada, deben ser trazables y auditables, y proceder de una fuente verificada, transparente, inteligible, contrastada y objetiva. En todo caso, además, ha de preservarse la confidencialidad mediante técnicas de anonimización, seudonimización o disociación y desagregación.

El Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), en su art. 22, establece el derecho de todo interesado (las partes en el caso del proceso judicial) a «no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar». Por tanto, el empleo de IA en el ámbito procesal penal afecta significativamente y produce efectos jurídicos sobre las partes como elemento que sirva para aportar datos a valorar por el juez. Establece, por tanto, el precepto de referencia, un derecho de reserva por el afectado para no ser objeto de una decisión automatizada y basada únicamente en IA cuando esta le afecta jurídicamente, si no consiente expresamente a ella.

Todo lo anteriormente expuesto nos lleva a concluir respecto de la anunciada segunda cuestión, que la función primordial de la IA ha de ser asistencial, nunca sustitutiva, de aquella que desarrollan todos y cada uno de los profesionales jurídicos concernidos: judicatura, fiscalía, colaboradores y auxiliares de los titulares de los órganos jurisdiccionales, abogacía y procura. Más aún cuando una razón de peso de estricto tenor dispuesto por el principio de legalidad que rige las actuaciones procesales considera de forma clara: no hay norma legal actualmente, al menos en España, que habilite la posibilidad de intervención y desempeño de un robot o una IA en las respectivas funciones profesionales en el proceso judicial de los miembros de la judicatura, la fiscalía, la abogacía o la procura, siendo además la normativa que rige cada una de estas profesiones jurídicas explícitamente referenciadas a personas físicas. Sin ir más allá en la reflexión, cuando menos atrevida y pavorosa, de plantear dejar la justicia, y lo que ello supone en cuanto a decidir sobre los derechos fundamentales de las personas, encomendada a máquinas y tecnología.

2. EXIGENCIAS PARA APLICAR INTELIGENCIA ARTIFICIAL EN LA LABOR JURISDICCIONAL

Asumiendo que el progreso tecnológico es un fenómeno irreversible, posiblemente el mejor avance que pueda ofrecerse en el ámbito procesal para encontrar acomodo a la IA y su aplicación en la labor

jurisdiccional sea disponer y explicitar las exigencias que su utilización conllevaría para realizarse dentro de un contexto garantista y eficiente. Tres son, a nuestro entender, las exigencias que podrían ser necesarias para una aplicación garantista de la IA en el ámbito procesal:

- a) Existencia de normativa legal de cobertura,
- b) Jurisdiccionalidad (control judicial salvo en los supuestos de herramientas predictivas en el ámbito de la investigación policial que no afecten derechos fundamentales y se basen en datos públicos),
- c) Respeto a los derechos fundamentales.

En el ecosistema legislativo nacional, actualmente no disponemos de una norma específica que regule la utilización de herramientas de IA en el ámbito procesal penal, si bien sí podemos acudir a algunas referencias genéricas en el empleo de estas soluciones tecnológicas en el ámbito de la Administración de Justicia. De este modo, acudiendo a la LOPJ, en su art. 236 (reformado por LO 7/2021) se sientan las bases para el posible empleo de soluciones tecnológicas —IA incluida— en juzgados y tribunales en relación con la obtención y tratamiento de datos en el ejercicio de la función jurisdiccional y la clasificación de decisiones en automatizadas, proactivas y asistenciales. Dicho precepto ha encontrado continuidad en la LO 15/2022, en cuyo art. 23 se habilita el empleo de IA y mecanismos de toma de decisión automatizados dentro de todas las Administraciones públicas «para que los algoritmos involucrados... tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente». De forma más directa y particular, en relación con el proceso penal y la obtención y tratamiento de datos, ha de tenerse en cuenta el articulado de la LO 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Finalmente, conviene recordar, como antecedente normativo que pudiera servir de referencia en actuaciones legislativas futuras, el tratamiento que para la implantación y utilización de IA en el proceso penal con diferentes fines, se ofrecía en el abortado Anteproyecto de Ley de Enjuiciamiento Criminal presentado en 2020, texto del cual pueden citarse como referencias a este respecto los arts. 368 —datos obrantes en archivos automatizados de los prestadores de servicios—, 485 —instrumentos de valoración del riesgo o reincidencia— y 516 a 520 —diligencias de investigación con utilización de datos—. Previsión que ha tenido continuidad en el reciente Proyecto de Ley de Enjuiciamiento Criminal, presentado en noviembre de 2025, en los arts. 366, 491 y 518 a 523.

Ciertamente, pudieran considerarse, como incipiente y verdadera referencia posible a nivel normativo en la incorporación de soluciones

de IA en el entorno procesal, y con carácter general, las previsiones del Real Decreto Ley 6/2023 (de 19 de diciembre, *BOE* de 20 de diciembre de 2023) determinando la posible utilización de herramientas de IA desde los objetivos definidos³ en su art. 1.3, el principio general de orientación de la justicia al dato⁴ [art. 35.k)] y la previsión de realización de posibles actuaciones automatizadas, proactivas y asistidas en la Administración de Justicia —con herramientas de IA— según lo dispuesto en los arts. 56, 57 y 58 del RDL 6/2023. Desde un marco legal amplio habilita, primeramente, en el art. 56, la instauración en la Administración de Justicia, de las que conceptúa como «actuaciones automatizadas», entendidas como aquellas actuaciones procesales producidas por un sistema de información adecuadamente programado sin necesidad de intervención humana en cada caso singular. Ofrece el precepto, la cobertura legal para que los sistemas informáticos utilizados en la Administración de Justicia posibiliten la automatización de las actuaciones de trámite o resolutorias simples, que no requieren interpretación jurídica, como puedan ser, en la enumeración orientativa que explicita: *a)* el numerado o paginado de los expedientes, *b)* la remisión de asuntos al archivo cuando se den las condiciones procesales para ello, *c)* la generación de copias y certificados, *d)* la generación de libros, *e)* la comprobación de representaciones, o, *f)* la declaración de firmeza, de acuerdo con la ley procesal.

De un tenor muy similar, por la ausencia de intervención humana directa en su producción, son las catalogadas, en segundo lugar, como actuaciones proactivas (art. 56.3 RDL 6/2023) considerando en este tipo de actuación con utilización de IA en la Administración de Justicia aquellas autoiniciadas por los sistemas de información sin intervención

³ Precepto que aportaría los requisitos de norma legal de cobertura y jurisdiccionalidad además de exigir el respeto a los derechos fundamentales, las tres exigencias que consideramos imprescindibles para la implementación garantista de soluciones de inteligencia artificial en el proceso. «Artículo 1. Objeto y principios. 1. La presente ley regula la utilización de las tecnologías de la información en el ámbito de la Administración de Justicia y en las relaciones de la Administración de Justicia con el resto de las administraciones públicas y sus organismos y entidades vinculadas y dependientes. 2. En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente ley, asegurando la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación, portabilidad e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones. 3. Las tecnologías de la información en el ámbito de la Administración de Justicia tendrán carácter instrumental de soporte y apoyo a la actividad jurisdiccional, con pleno respeto a las garantías procesales y constitucionales».

⁴ Artículo 35 RDL 6/2023. «Todos los sistemas de información y comunicación que se utilicen en el ámbito de la Administración de Justicia, incluso para finalidades de apoyo a las de carácter gubernativo, asegurarán la entrada, incorporación y tratamiento de la información en forma de metadatos: *k)* La aplicación de técnicas de inteligencia artificial para los fines anteriores u otros que sirvan de apoyo a la función jurisdiccional, a la tramitación, en su caso, de procedimientos judiciales y a la definición y ejecución de políticas públicas relativas a la Administración de Justicia».

humana, que aprovechan la información incorporada en un expediente o procedimiento de una Administración pública con un fin determinado, para generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración pública, en todo caso conformes con la ley.

Unas —actuaciones automatizadas— y otras —actuaciones proactivas— comparten como comunes denominadores el que de ser implantadas en los sistemas de la Administración de Justicia asegurarán: *a)* que todas las actuaciones automatizadas y proactivas se puedan identificar como tales, trazar y justificar, *b)* que sea posible efectuar las mismas actuaciones en forma no automatizada, *c)* que sea posible deshabilitar, revertir o dejar sin efecto las actuaciones automatizadas ya producidas.

En último término, se prevé normativamente también la posibilidad de implantar actuaciones asistidas en la Administración de Justicia (art. 57 RDL 6/2023), presentando esta posibilidad de utilización auxiliar de sistemas de inteligencia artificial el importante rasgo diferencial con las anteriores de condicionar su validez al refrendo por humano. Define la norma este tipo de actuaciones como «aquella para la que el sistema de información de la Administración de Justicia genera un borrador total o parcial de documento complejo basado en datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal». Quedando meridianamente destacado su carácter auxiliar, no decisorio o resolutivo *per se*, por cuanto en ningún caso el borrador documental así generado constituirá por sí una resolución judicial o procesal, sin validación de la autoridad competente. Los sistemas de la Administración de Justicia asegurarán que el borrador documental solo se genere a voluntad del usuario y pueda ser libre y enteramente modificado por este. Constatación desde la propia norma reguladora de la observancia del principio de control por humano, como principio capital en la utilización de IA con carácter general, y de forma expresa y particular en este supuesto. Circunstancia que se remarca explícitamente en el último párrafo del precepto al disponer que la constitución de resolución judicial o procesal requerirá siempre la validación del texto definitivo, por el juez o jueza, magistrado o magistrada, fiscal o letrado o letrada de la Administración de Justicia, en el ámbito de sus respectivas competencias y bajo su responsabilidad, así como la identificación, autenticación o firma electrónica que en cada caso prevea la ley, además de los requisitos que las leyes procesales establezcan.

En el entorno particular de la justicia penal, y la implementación de soluciones tecnológicas de IA, sería deseable que desde estas muy generalistas bases normativas que acabamos de referir, se aportase un marco normativo específico, claro y determinado, ya sea en el con-

tenido de la LECrim —mediante su reforma o la promulgación de un nuevo texto—, ya sea mediante una ley específica de implementación de la IA como elemento auxiliar en el proceso penal, pero en todo caso desde una norma con rango de ley orgánica por la directa afectación que su incorporación a la legalidad conlleva con los derechos fundamentales de las personas.

Finalmente, cabe aludir a la segunda de las exigencias que acreditarían y legitimarían la implementación de soluciones de IA con destino al proceso, como es el requisito de la jurisdiccionalidad, desde una doble y concordante vertiente. De inicio, porque comportaría el cumplimiento escrupuloso del principio, ya consabido, de control por humano en la aplicación de la IA, siendo los titulares de los órganos jurisdiccionales quienes decidirían, supervisarían y, en su caso, asumirían los resultados de la utilización de las citadas herramientas. Además, como elemento humano garante de la salvaguarda de las garantías y derechos fundamentales en la aplicación de la IA en el proceso, responsabilidad y competencia atribuida también a los órganos jurisdiccionales, únicos depositarios de la facultad constitucional de afectación a los derechos fundamentales de los ciudadanos cuando así proceda, siempre de forma proporcional y motivada.

3. DERECHOS Y GARANTÍAS PROCESALES: INSERCCIÓN EN LA APLICACIÓN DE INTELIGENCIA ARTIFICIAL A LA JUSTICIA PENAL

La implementación de sistemas de inteligencia artificial en el ámbito procesal, sobremanera en el del proceso penal, requiere de la observancia de las máximas garantías para el justiciable. Incorporar sistemas expertos tecnológicos en funciones asistenciales o auxiliares de la labor de los operadores jurídicos, particularmente en la atribuida a los titulares de los órganos jurisdiccionales, ha de ser plenamente respetuoso con los derechos fundamentales, tal y como señalábamos en el apartado precedente al disponer las tres exigencias incuestionables para la utilización garantista de IA en la Administración de Justicia. A esta exigencia general, debe sumarse un punto de particular y escrupuloso cumplimiento ante los derechos fundamentales procesales: derecho a la tutela judicial efectiva, derecho de defensa, presunción de inocencia y derecho al debido proceso.

Si en relación con los derechos fundamentales en general se asume como uno de los principios básicos de la utilización de IA la condición de que su diseño y aplicación sean absolutamente compatibles y totalmente respetuosos con los derechos fundamentales, más importancia cobra, aún, la singularidad en relación con los derechos fundamentales procesales, tal y como ya anticipó la Agencia Europea de Derechos

Fundamentales en su documento «Big Data: Discrimination in data-supported decision making» (2018) estableciendo de forma expresa y tajante que «el uso de nuevas tecnologías y algoritmos, incluido el *machine learning* y la *inteligencia artificial*, afecta a varios derechos fundamentales, entre ellos, sin que se limite solo a dichos derechos: el derecho a un juicio justo, la prohibición de discriminación, el derecho a la intimidad, la libertad de expresión y el derecho a un recurso efectivo». Circunstancia que ratificó el Consejo de Europa en su «European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment» (2018) explicitando que «el uso de herramientas y servicios de IA en los sistemas judiciales tiene como objetivo mejorar la eficiencia y la calidad de la justicia y merece ser fomentado. Sin embargo, debe hacerse de forma responsable, respetando los derechos fundamentales de las personas, tal como se establecen en el Convenio Europeo de Derechos Humanos (CEDH) y el Convenio núm. 108 del Consejo de Europa sobre la Protección de Datos de Carácter Personal, así como los demás principios fundamentales establecidos en la Carta».

Con estos precedentes, el asentamiento del eventual empleo de las herramientas de IA, ya sea en su máxima extensión configurando un medio de prueba el resultado de su aplicación o como instrumento de predicción o asistencia en la valoración de determinadas situaciones procesales penales como pueda ser el resultado de diligencias de investigación, pasa inexorablemente por el pleno respeto a los derechos fundamentales procesales comprometidos y desde la exigencia del respeto a las máximas garantías para el justiciable.

Quizá, como primera salvaguarda, no debiera olvidarse la necesidad de que sea «visible» que estamos interactuando con una IA, ciertamente en funciones asistenciales y que precisará del refrendo por humano. Prestemos atención, entonces, a las consideraciones del Consejo de Europa, pionero en abordar a nivel de tratado internacional jurídicamente vinculante las consecuencias de la IA en aras de garantizar el respeto de los derechos humanos, del Estado de derecho y las normas jurídicas democráticas en el uso de los sistemas de IA, mediante el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho (2024). El art. 15 del citado Convenio hace alusión directa a las garantías procesales, reclamando que cada Estado parte garantice que cuando un sistema de inteligencia artificial tenga un impacto significativo en el disfrute de los derechos humanos, las personas afectadas por el mismo dispongan de garantías procesales, salvaguardias y derechos efectivos, de conformidad con el derecho internacional y nacional aplicable. Y siempre, prosigue, velando por que, según corresponda al contexto, se notifique a las personas que interactúan con sistemas de inteligencia

artificial que están interactuando con dichos sistemas en lugar de con un ser humano.

Cuatro son, al menos y como ya hemos resaltado con antelación, los derechos procesales fundamentales comprometidos y afectados de forma directa e inmediata por la incorporación de sistemas de inteligencia artificial a las actuaciones con trascendencia procesal penal.

3.1. El derecho a la tutela judicial efectiva

Una de las proyecciones que la jurisprudencia constitucional ha conferido al derecho a la tutela judicial efectiva es el acceso a los órganos jurisdiccionales, que ha de mantenerse expedito y sin condiciones o requisitos inhabilitantes a favor del justiciable. La utilización de herramientas de inteligencia artificial en cuestiones procesales penales no puede ser condición o requisito que menoscabe el libre acceso por parte del ciudadano a los juzgados y tribunales para obtener tutela judicial de sus derechos. Derivar a herramientas tecnológicas de este cariz, que elaboren planteamientos criminales predictivos, no puede impedir o propiciar que un ciudadano se retraiga de plantear su asunto judicialmente y obtener la pertinente tutela de sus derechos por parte de los órganos jurisdiccionales competentes.

En aquellos supuestos en que el órgano jurisdiccional pudiera recurrir a un sistema inteligente para la preparación, motivación o elaboración de su resolución será absolutamente imprescindible que dicha decisión esté fundada en derecho y motivada para cumplir con las exigencias inherentes al derecho a la tutela judicial efectiva. Ha de conocerse la «razonabilidad», motivación y congruencia de la decisión, su correlación con el objeto del proceso (hechos y pretensiones) y el contraste con la operación algorítmica llevada a cabo, sin perjuicio de que en el caso de tratarse de inteligencias artificiales en funciones asistenciales o predictivas (o de actividades policiales de investigación penal cuya valoración posterior corresponda al órgano jurisdiccional), quede en manos del juzgador (control humano, como una de las premisas indisociables a la IA) el encaje de la lógica tecnológica con la resolución que dicta y asume como propia. La Resolución de 16 de febrero de 2017 del Parlamento Europeo prevé, en relación con esta cuestión, en su Considerando H, que ha de velarse por la inteligibilidad de los procesos decisorios de las herramientas de inteligencia artificial, cuestión que concuerda directamente con la necesidad insoslayable de fundar en derecho y motivar una resolución jurisdiccional, también obtenida con apoyo o aplicación plena de IA. Más recientemente, el Reglamento Europeo de 2024 sobre inteligencia artificial, al considerar estos sistemas como de alto riesgo en el ámbito de la Administración de Justicia, corrobora la necesidad de observancia

plena de este derecho fundamental por cuanto afecta a la propia democracia, el Estado de derecho y la justicia.

3.2. El derecho de defensa

El acceso y empleo de herramientas de IA, salvo que se dispongan de forma pública e igualitaria desde instituciones públicas, requiere un desembolso económico por cuanto se trata de creaciones informáticas procedentes, generalmente, de empresas privadas. Es por ello que, en primer término, y en vinculación directa con el derecho a la igualdad, podrían producirse desequilibrios en los casos en que una de las partes utilice herramientas de IA para la preparación del asunto (en el entorno del actualmente denominado *legaltech*) frente a aquella otra que no tenga a su alcance los recursos (económicos o materiales) para ello, por cuanto le permitirá al litigante que la emplea desplegar con mayor eficiencia sus argumentos (más datos, más comparativas, etc.). En igual sentido en cuanto a garantizar un derecho de defensa efectivo, ante el posible rechazo de un abogado a la defensa de un asunto cuando un previo cálculo predictivo de posibilidades arroje un resultado de posible éxito muy bajo o pobre. De ahí que en el ámbito procesal penal sea recomendable su empleo a nivel jurisdiccional público.

En segundo lugar, el derecho de defensa se puede ver afectado cuando se desconoce el funcionamiento de la herramienta de inteligencia artificial, bien porque no se le notifica o bien porque no se le otorga información suficiente al afectado, y no se presta un consentimiento informado y con garantías, sobre sus características y funcionamiento, así como si no se traslada al órgano jurisdiccional y a las partes el diseño y funcionamiento del programa y sus algoritmos (*black box*). Esta situación dará lugar a indefensión a las partes por hurtarles el conocimiento de la forma en que se ha obtenido el resultado o la predicción. Incluso podría llegar a extenderse hasta la consideración de si, con la utilización de aplicaciones de esta naturaleza tecnológica, y desde el respeto al derecho de defensa, podría vulnerarse de algún modo su vinculación con la utilización de medios de defensa y de prueba pertinentes y lícitos, si no hay una regulación legal previa que establezca las condiciones y límites para su uso en el proceso penal. Este inconveniente al derecho de defensa, y que se garantice un uso de IA en el proceso de forma adecuada y acorde con los derechos fundamentales procesales, exige detallar a las partes el procedimiento de automatización de forma explicable y cognoscible más allá de su justo resultado, para así descartar legítimamente todo riesgo de ausencia de transparencia, carencia de control humano, ausencia de confidencialidad o riesgo de sesgo o discriminación.

Como posibles soluciones, que puedan garantizar entonces el derecho de defensa, se plantean dos opciones. La primera opción es la transparencia técnica completa (por ejemplo, el código fuente abierto y la documentación y datos empleados), circunstancia que topa con el hecho de que, a veces, está restringida por la protección de secretos comerciales, propiedad intelectual o propiedad industrial de productos registrados. Ante ello, la única salida podría ser la utilización en el ámbito de la Administración de Justicia de herramientas de inteligencia artificial de carácter público o bajo control público, para garantizar la transparencia. Como segunda alternativa, podría contemplarse el lograr un equilibrio entre la propiedad intelectual de ciertos métodos de procesamiento y la necesidad de transparencia (acceso al proceso de diseño), imparcialidad (ausencia de sesgo), e integridad intelectual (priorizar los intereses de la justicia) cuando se utilizan herramientas tecnológicas que pueden tener consecuencias legales.

Así, jurisprudencialmente ya se ha dilucidado sobre esta segunda alternativa. Pueden referenciarse en apoyo de la misma dos asuntos ventilados ante los órganos jurisdiccionales norteamericanos, los casos *State v. Pickett* (2021) y *New Jersey v. Francisco Arteaga* (2023). En la resolución del primero, *State v. Pickett*, de 3 de febrero de 2021, Superior Court of New Jersey Appellate Division. 466 N.J. Super. 270 (App. Div. 2021), se trae causa del cuestionamiento de un *software* novedoso en HD para genotipificación probabilística para pruebas de ADN. El Tribunal de New Jersey considera que cuando están en juego las libertades civiles la revisión independiente del código fuente es fundamental para determinar la fiabilidad, y que, en caso de una tecnología novedosa, el demandado tiene derecho a acceder a la misma a través de una petición de descubrimiento con orden de protección siempre que: 1) exista una base racional para la petición apoyada por un experto, 2) se solicite una información específica, 3) se pueda salvaguardar la propiedad intelectual mediante orden de protección 4) concorra cualquier otro factor relevante. Jurisprudencia que refuerza el asunto *New Jersey v. Francisco Arteaga* (EEUU), de 7 de junio de 2023, Superior Court of New Jersey, Appellate Division Docket n.º A-3078-21, donde se ha admitido el acceso al código fuente mediante una orden de protección de revisión a puerta cerrada del código fuente y los materiales recibidos. Se solicita el «descubrimiento» de la tecnología de reconocimiento facial (FRT) para identificación del sospechoso en robo con arma de fuego en una tienda a partir de que, supuestamente, el gerente de la tienda lo habría reconocido de una visita anterior. Al descubrir que la tecnología FRT tuvo un papel importante en la identificación del sospechoso por los testigos, la defensa solicitó su descubrimiento con el código fuente, sus tasas de error, rendimiento, sistema de puntuaciones, lista de parámetros, y otros extremos. Se acuerda pericial de experto, sobre posibles problemas de fiabilidad

y la razón de la necesidad del «descubrimiento» para evaluar sus resultados y rendimiento. De esta manera, se considera que la prueba solicitada está directamente vinculada con la defensa en la posibilidad de sembrar la duda razonable. Además, en el expediente había pocas pruebas sobre el sistema y la defensa del acusado resultó convincente en lo concerniente a la novedad del sistema y a la necesidad de evaluar su fiabilidad.

3.3. El derecho a la presunción de inocencia

Puede verse desvirtuado, más aún por su importancia en el ámbito del proceso penal siendo capital para el investigado o encausado, cuando el sistema de inteligencia artificial aplicado en actividades de posible perfilación, identificación, investigación o valoración de riesgo, prueba, etc. es discriminatorio y sesgado en relación con determinados perfiles de personas por su origen, condición, raza, género, lugar de residencia e, incluso, debido a ostentar posibles antecedentes penales. Incluso, puede generarse un efecto pernicioso sobre la presunción de inocencia en virtud del manejo de datos o hechos desarraigados del proceso y totalmente ajenos al mismo que puedan perjudicar al investigado o encausado, como puedan ser los de tipo socioeconómico, laboral o educativo (entre otros). Dilucidar sobre la culpabilidad o inocencia de una persona no es una mera cuestión de perfilación automática sobre patrones preestablecidos por un sistema de inteligencia artificial, siempre y en todo proceso penal hay una diferencia concurrente: los hechos y las circunstancias de posible comisión del hecho delictivo. No hay dos hechos delictivos iguales y las previsiones que pueden arrojar millones de datos y los algoritmos más evolucionados no pueden condicionar la presunción de inocencia que requiere la existencia de pruebas de cargo concluyentes, legales e indubitadas. E, incluso, podría ser lesivo con el derecho a la presunción de inocencia el empleo de herramientas que cuestionen la defensa del investigado o encausado, por ejemplo, contraponiendo o contrastando la veracidad de sus declaraciones, cuando jurisprudencialmente se admite sin ambages, por ejemplo, el derecho a mentir del investigado o encausado como estrategia de defensa, que podría verse desvirtuada, conjuntamente con la presunción de inocencia, el derecho a no declarar y a no confesarse culpable, si recurriésemos, por ejemplo, a una solución de inteligencia artificial que determine la probabilidad de veracidad o falsedad de las declaraciones del investigado.

3.4. Derecho al debido proceso

Desde la amplitud que abarca el derecho al debido proceso, el empleo de utilidades de IA vinculadas a diligencias de investigación, o en materia probatoria, incide directamente, de nuevo y entre otras consecuencias, en el máximo respeto a las exigencias de igualdad y contradicción entre las partes en el proceso penal, así como también con respecto a las exigencias anteriormente referidas del Reglamento General de Protección de Datos europeo relativas a que tanto el juzgado o tribunal como los litigantes conozcan los datos y algoritmos empleados por el sistema a la hora de evacuar su resultado o propuesta. Derivación natural del derecho al debido proceso es la interrelación con la exigencia constitucional del juez ordinario predeterminado por la ley. Se trata, desde uno y otro, de eliminar y proscribir arbitrariedades en el proceso judicial. Llegados a este punto, puede asaltar-nos la duda de si el empleo de inteligencias artificiales pudiera afectar el derecho al juez ordinario predeterminado por la ley, en cuanto es un elemento no inicial del proceso, condicionado a una elección subjetiva, cuando el derecho al juez ordinario predeterminado por la ley, de suyo, se refiere a un juez humano. Además, la utilización de IA en el ámbito procesal penal, como hemos señalado, debe venir sostenida sobre una previa habilitación legal de cobertura, para dar cumplimiento a la exigencia constitucional y procesal de legalidad (arts. 9.3 CE y 1 LECrim).

4. PRINCIPIOS RECTORES

Ante un desafío, como es la exigencia de garantías frente a eficiencia en la implementación de sistemas de inteligencia artificial en el ámbito del derecho procesal penal, asumen un protagonismo descolante una serie de principios rectores en su aplicación. Tomamos para ello, como referencia, los enunciados en el Código Ético Europeo del Consejo de Europa (2018), refrendados posteriormente por la Unión Europea (2019) en su documento «Pautas éticas de confianza en inteligencia artificial». Estos son:

a) Principio de respeto a los derechos fundamentales: asegurando que el diseño y la aplicación de herramientas y servicios de IA son totalmente compatibles y respetuosos con los derechos fundamentales. En nuestro caso, cuando se utilizan herramientas de IA en la investigación policial, instrucción y enjuiciamiento de delitos, es esencial garantizar que no socavan las garantías del derecho de acceso al juez (tutela judicial efectiva), derecho de defensa, derecho a un juicio justo (igualdad y contradicción) y derecho a la presunción de inocencia.

b) Principio de no discriminación: tendente a evitar la aparición o intensificación de cualquier tipo de discriminación o estigmatización entre individuos o grupos de personas por cuanto se manejan datos muy sensibles. Debe huirse de la utilización de análisis deterministas —prejuicios— que «prejuzguen a determinados colectivos por razón de sexo, opinión, creencia, afiliación política o sindical, datos genéticos o biométricos, orientación sexual» o, por ejemplo, a un reincidente. Sin duda, es uno de los elementos que desde la utilización del *big data*, y su aplicación a mecanismos de decisión a través de IA, más directamente incide en la posible lesión de derechos fundamentales, tanto a nivel general como a nivel singular procesal, requiriendo con ello las máximas garantías en su aplicación en situaciones procesales.

c) Principio de calidad y seguridad: particularmente necesario respecto al procesamiento de decisiones y datos judiciales, utilizando fuentes certificadas y datos intangibles (modelos elaborados de manera multidisciplinar, en un entorno tecnológico seguro, compatibles con las exigencias normativas de protección de datos personales). Los modelos y algoritmos creados también deben poder almacenarse y ejecutarse en entornos seguros, a fin de garantizar la integridad e intangibilidad del sistema (evitando el peligro de manipulaciones, hackeos, etc.).

d) Principio de transparencia e imparcialidad: haciendo accesibles y comprensibles los métodos de procesamiento de datos y habilitando la realización de auditorías externas. Se debe garantizar la ausencia de sesgo o discriminación en el funcionamiento del sistema de IA, determinando con ello su imparcialidad.

e) Principio de «control por el usuario»: excluye un enfoque prescriptivo y garantiza que los usuarios sean actores informados y que asuman el control de las decisiones tomadas. En nuestro caso, produciría que los profesionales del sistema de justicia penal deban asumir o revisar las valoraciones o propuestas emitidas por una solución de IA y los datos utilizados para generar un resultado (elemento de supervisión humana en todo caso y en último término). Finalmente comprendería también el que podríamos denominar como «derecho a objetar», cuando el sujeto afectado, y previa información del empleo de sistemas de IA, durante un proceso judicial, solicite que su situación o resolución se efectúe directa y exclusivamente por un juzgado o tribunal y no de forma automatizada —situación que, recordamos, contempla el art. 57 del RDL 6/2023 en relación con las actuaciones automatizadas o proactivas que puedan implantarse en la Administración de Justicia—.

Exigencia que también se cristaliza, más recientemente, en el art. 14 del Reglamento de la Unión Europea sobre Inteligencia Artificial (2024), en cuyo apartado segundo refrenda la importancia de la supervisión humana de los mecanismos de IA precisando y concretando que el objetivo de la supervisión humana será prevenir o reducir

al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de inteligencia artificial de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible. Serán, en nuestro caso, y como ya hemos apuntado con la exigencia de jurisdiccionalidad, los titulares de los órganos jurisdiccionales quienes, en el ámbito de la Administración de Justicia, deben, en cualquier momento, poder revisar los datos, algoritmos y criterios de tratamiento utilizados para producir un resultado en la utilización de una IA con destino a las actuaciones o resoluciones procesales, y seguir sin estar necesariamente vinculados por ellos a la luz de las características específicas de ese caso en particular.

5. POSIBILIDADES Y CONDICIONES

Con carácter previo a la exposición de algunas de las aplicaciones judiciales de IA en el ámbito procesal penal, hemos de reiterar que en todo caso se basan, como cualquier otra de similar naturaleza y diseño tecnológico, en un conglomerado de datos que pertenecen al pasado, por tanto, pueden llegar a suponer un cierto obstáculo para el avance del derecho. El automatismo de las decisiones predictivas aporta un riesgo de estandarización de pautas y argumentos jurídicos implicando, indirectamente y a medio plazo, la eliminación de los criterios de interpretación, lo que podría conllevar a resultados indeseados, erráticos e insatisfactorios en algunos casos por cuanto pueden perpetuar, reforzar o exacerbar la discriminación y sesgos existentes, incluidos los estereotipos, los prejuicios o las desigualdades estructurales, y posibilitar una toma de decisiones distorsionada u opaca, con vulneración de otros derechos fundamentales como la dignidad humana, el derecho a la libertad, la no discriminación, la privacidad y la protección de datos.

Surge el debate acerca de la idoneidad, entonces, de estas aplicaciones disruptivas de cara a la labor jurisdiccional. En algunos casos, se admite, con menores reservas, su aplicabilidad a situaciones procesales basadas en criterios estrictamente comparativos de elementos objetivos —pretensión— y subjetivos —parte activa y pasiva del proceso— como pueden ser los casos de valoración del efecto de cosa juzgada, acumulación de procesos, litispendencia, cálculo de acumulación de condenas, etc. Además, se plantea la duda de si el algoritmo que rige una IA ha de basarse en la cantidad —número de resoluciones coincidentes— o en la jerarquía —resoluciones de los órganos de superior categoría, aunque sean menores en número—. Finalmente, en el empleo de herramientas de IA por órganos jurisdiccionales, en funciones asistenciales: ¿es controlable su utilización jurisdiccional vía «impugnación» garantizando con ello el dere-

cho a la tutela judicial efectiva en su vertiente de derecho al recurso? Es evidente, en este caso, la necesidad de disponer de un sistema adecuado y eficaz para el seguimiento y la revisión de las aplicaciones de IA y sus resultados.

A partir de estas indispensables consideraciones preliminares, son múltiples los usos que puede tener la IA para el órgano jurisdiccional. Tanto en tareas procedimentales, relacionadas con la sistematización y la clasificación y ordenación de documentación, como en sistemas de valoración del riesgo de cara a la adopción de determinadas medidas (cautelares, ejecución de sentencia, incidencias en el régimen penitenciario) o en elementos de valoración de determinadas diligencias o pruebas en relación con su licitud, objetividad, pertinencia o resultados (credibilidad del testimonio, adecuación del perito y del informe pericial, etc.). Si tratamos de concretar aún más la cuestión, pueden servir como hoja de ruta las Recomendaciones de uso de inteligencia artificial que presentó el Consejo de Europa (2018) en relación a la justicia (ECUIA in Justice), distribuyéndolas en cuatro categorías en función del criterio de su grado de idoneidad para concretas actividades procesales. Así, en primer lugar, considera que estas aplicaciones son muy recomendables para: *a)* mejora del análisis y estructuración de la jurisprudencia, *b)* acceso al contenido de normas legales, *c)* creación de nuevas herramientas estratégicas. En segundo lugar, establece que puede ser idónea, requiriendo considerables precauciones metodológicas, en los casos cuya finalidad sea: *a)* ayuda en la elaboración de escalas/baremos en determinados conflictos civiles, *b)* apoyo a medidas alternativas de solución de controversias en materia civil, *c)* ODR, *d)* uso de algoritmos en la investigación criminal para identificar dónde y cómo se cometen los delitos penales. En tercer lugar, y aumentando paulatinamente el grado de reserva en su utilización, determina posibles usos, a considerar después de estudios científicos adicionales que avalen su nivel de garantías en los casos en que el empleo de soluciones de IA en el proceso tenga como objetivo: *a)* la determinación del perfil del juez/tribunal y *b)* la anticipación de decisiones judiciales (justicia predictiva). Finalmente, en último lugar, muestra el nivel de reserva más extrema a su empleo en relación con el uso de algoritmos en materia penal para la perfilación de personas.

Desde estas pautas, conviene conectar las reflexiones anteriores, al analizar las posibilidades y condiciones del empleo de herramientas de inteligencia artificial en el proceso penal con las disposiciones más cercanas temporalmente, esto es, con el Reglamento Europeo de Inteligencia Artificial de 2024, que establece como puntos clave, entre otros, los supuestos expresamente prohibidos de uso de IA, y dentro de los cuales concurren algunos directa, o indirectamente, relacionados con nuestra materia. Dentro de las seis grandes prohibiciones

de uso de IA que refiere el art. 5 del precitado Reglamento⁵ (categorización biométrica con características sensibles; scraping generalizado de imágenes faciales de internet o CCTV para generar bases de datos de reconocimiento facial; reconocimiento de emociones en entornos laborales y educativos; sistemas de scoring social basado en comportamiento o características personales; sistemas de manipulación subliminal; y sistemas que exploten vulnerabilidades de las personas: edad, discapacidad, situación social, económica), concretamente los apartados *d)*, *g)*, *h)* y anexo III apartado 6, se vinculan a un supuesto relacionado con aplicaciones procesales penales de sistemas de identificación biométrica en espacios de acceso público con fines policiales, que se habilita, excepcionalmente, previa autorización judicial y para determinados delitos. Obsérvese cómo concurre en esta excepción la exigencia de jurisdiccionalidad que hemos seleccionado como imprescindible para la implantación de soluciones de IA en el ámbito de la justicia, aunada a su previa consideración normativa —también, a nuestro parecer, como otro de los requisitos ineludibles—.

En este contexto, el Reglamento permite la utilización de sistemas de identificación biométrica «a distancia» solo estrictamente en la búsqueda selectiva de una persona condenada o sospechosa de haber cometido un delito grave o bien para proceder a una identificación «en tiempo real» limitados a: *a)* búsquedas específicas de víctimas (secuestro, trata, explotación sexual), *b)* prevención de una amenaza terrorista específica y actual, o, *c)* la localización o identificación de una persona sospechosa de haber cometido uno de los delitos específicos mencionados en el propio Reglamento (por ejemplo, terrorismo, trata de seres humanos, explotación sexual, asesinato, secuestro, violación, robo a mano armada, participación en una organización delictiva, delitos contra el medio ambiente). Se establece, asimismo, la concurrencia del tercer factor de relevancia que señalábamos en el apartado segundo del presente estudio, el respeto a los derechos fundamentales, por cuanto el art. 27 del Reglamento de inteligencia artificial de la Unión Europea de 2024, obliga a los implementadores de sistemas de IA de alto riesgo a realizar una evaluación de impacto (FRIA, por sus siglas en inglés, «fundamental rights impact assessment»), entre otras obligaciones específicas.

Descendiendo a un plano más práctico y operativo, disponemos ya de referencias reales e implementadas con diversos fines, como son los casos de STEVIE (solución que plantea hipótesis coherentes

⁵ Véase también el documento «Anexo de la Comunicación a la Comisión. Aprobación del contenido del proyecto de Comunicación de la Comisión - Directrices de la Comisión sobre prácticas prohibidas en materia de inteligencia artificial establecidas por el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial) de 4 de febrero de 2025, referencia: C(2025) 884 final».

utilizando los datos de una investigación), PEIRCE-IGTT (plantea hipótesis de la acusación y la defensa), Alibi (pronostica el comportamiento defensivo de los encausados y sus posibles explicaciones ante un delito), COMPAS (valoración de riesgo de reincidencia por el investigado), Questmap, Argumed o Cato (ayudan a estructurar argumentos jurídicos), Casecrunch (predicción de resultados) Probation and Pretrial Service Office (PTRA) o Public Safety Assessment (PSA) (destinados a la realización de valoraciones criminológicas). A nivel nacional pueden referirse soluciones de IA en este ámbito como: Calculadora 988 (cálculo de acumulación de condenas), RISCANVI (valoración de la probabilidad de reincidencia de presos ante solicitud de permiso penitenciario), o la robotización y automatización de cancelación de antecedentes penales.

La innovación más reciente la ha planteado el Gobierno de la Generalitat de Cataluña impulsando una iniciativa con funciones asistenciales en la elaboración de resoluciones jurisdiccionales, denominada proyecto AI4Justice. Desde su consideración de herramienta de apoyo a la función jurisdiccional, ofrece la posibilidad de automatización de tareas judiciales repetitivas y estructuralmente predecibles. Inicialmente, en la fase de pruebas, se está testando en relación con litigios específicos considerados de poca complejidad jurídica (reclamaciones derivadas de retrasos o cancelaciones de vuelos y litigios sobre cláusulas suelo en contratos de préstamo hipotecario) sobre la consideración de que son asuntos con hechos concurrentes y una línea jurisprudencial precedente homogénea. Sobre esa teórica previsibilidad se oferta esta herramienta de IA para la elaboración de borradores de resoluciones judiciales, sin comprometer la necesidad de una ponderación casuística o la singularidad del conflicto jurídico. Se han adoptado prevenciones, por parte de sus impulsores institucionales para que la herramienta únicamente tenga carácter auxiliar y asistencial, sin que elimine la labor jurisdiccional de interpretación de los hechos y sus consecuencias jurídicas, para evitar que pueda generalizarse un estatismo y estandarización no deseados desde «la dependencia de datos históricos y la recurrencia de estructuras argumentativas prediseñadas podrían condicionar *de facto* el razonamiento jurídico, homogeneizando las decisiones judiciales y limitando el margen de interpretación conforme a las circunstancias específicas de cada caso. Este riesgo se ve agravado por la posibilidad de que la IA actúe como un corsé interpretativo, especialmente si no se garantiza una supervisión humana activa y crítica, que permita modular, corregir o reorientar los borradores generados por el sistema».

Con evidentes connotaciones policiales, y de cuya labor como personal auxiliar del órgano jurisdiccional se pueden generar actuaciones procesales, particularmente importantes en el ámbito de la averiguación del delito y de la identificación de autores y víctimas, podemos contras-

tar la utilización de soluciones de IA con una doble función: predictiva y analítica en relación con el delito y sus posteriores consecuencias procesales. Pueden aportar a la labor policial la detección de patrones específicos de delincuencia o de comportamientos criminales desde el almacenamiento y tratamiento masivo de datos. La policía predictiva pasa, con ello, a ser una técnica policial más orientada al análisis y tratamiento de datos criminales para identificar objetivos, prevenir delitos y resolver los ya cometidos. De esta forma, a nivel internacional encontramos aplicaciones para la identificación biométrica (ADN, reconocimiento facial, etc.) como Cloud Walk (basada en reconocimiento facial y análisis de la marcha), Fast (analizando la frecuencia cardíaca o la firmeza de la mirada), ExpertCop o PDLC y Predpol (para predicción y elaboración de mapas criminales con identificación de hotspots —lugares de concentración de determinada delincuencia—), ROSSMO (que permite estimar el área geográfica donde es más probable que resida un presunto agresor en serie en función de la ubicación de los delitos que previamente se le han atribuido), Age-Progress Ware (para la localización de personas desaparecidas), o Valcri (para analizar toda la información obtenida en la escena del crimen y relacionarla con el proceder de criminales que han llevado a cabo delitos similares).

A nivel nacional hemos de hacer referencia, en el ámbito de actuación policial con herramientas de IA, a la implementación de Veripol (para la valoración de la veracidad de denuncias presentadas en Comisaría) y de VioGén (sistema más completo, desarrollado y complejo de identificación, valoración y seguimiento de victimización en violencia de género a través de un cuestionario donde se registran una serie de factores de riesgo). Otros sistemas utilizados policialmente para diferentes funciones también son: SIG (Sistema de Información Cartográfica, para recopilar, representar y analizar elementos geográficos y de localización), CATT (herramienta de análisis en chat para la investigación de agresiones sexuales a menores a través de las redes sociales) o HATE (para investigación y seguimiento de delitos de odio en redes sociales). Se está abriendo paso también la utilización de las denominadas técnicas de «Inteligencia de fuentes abiertas» u Open Source Intelligence (OSINT) que hace referencia al conocimiento recopilado a partir de fuentes de acceso público y posteriormente aplicadas con herramientas de IA. El proceso incluye la búsqueda, selección y adquisición de la información, así como un posterior procesado y análisis de esta con el fin de obtener conocimiento útil y aplicable en distintos ámbitos (uso de IA en todas estas posibles situaciones). Fuentes abiertas a partir de las cuales se puede obtener información relevante, entre las que destacan: medios de comunicación: revistas, periódicos, radio; información pública de fuentes gubernamentales: foros, redes sociales, *blogs*, *wikis*; conferencias, simposios, papers, bibliotecas online, recursos publicados en *open access*.

Por el contrario, también existen sistemas de inteligencia artificial, utilizados en otros países, cuya dinámica y funcionamiento nos ofrecen muchas reticencias y reparos al no respetar absolutamente los derechos fundamentales. Son los casos, por ejemplo, de Palantir Gotham (sistema de inteligencia artificial que identifica criminales a partir de los patrones de comportamiento obtenidos de un análisis de los datos presentes en la red y de aquellos que están en manos de los poderes públicos y empresas privadas sin distinguir los datos que son de especial protección como podrían ser las huellas o el historial médico) y de Faception (diseñadores aseguran que puede definir el carácter de una persona con base a los rasgos de nuestro rostro y comportamiento, tras la observación de rostros en vivo, o a través de imágenes o videos para analizar distintos rasgos y clasificar a las personas en quince grupos ya definidos con el altísimo riesgo de sesgos y discriminación que esta técnica presenta).

6. BIBLIOGRAFÍA

- ARIZA COLMENAREJO, M. J. (2023), «Fuentes de datos al servicio de sistemas de inteligencia artificial dirigidos a la toma de decisiones judiciales», *Inteligencia artificial y proceso penal: Un reto para la justicia*, Cizur Menor: Aranzadi, pp. 15-42.
- BARONA VILAR, S. (2024a), «Justicia con algoritmos e inteligencia artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?», *Derechos y Libertades: Revista de Filosofía del Derecho y Derechos Humanos*, 51, pp. 83-115.
- (2024b), «El dilema del razonamiento, motivación y decisión judicial algorítmica (IA): ¿la posibilidad de lo imposible?», *Teoría & Derecho. Revista de pensamiento jurídico*, 37, pp. 150-175.
- BORGES BLÁZQUEZ, R. (2021), *Inteligencia artificial y proceso penal*. Cizur Menor: Aranzadi.
- BUENO DE MATA, F. (2022), «La necesidad de regular la inteligencia artificial y su impacto como tecnología disruptiva en el proceso: De desafío utópico a cuestión de urgente necesidad», en BUENO DE MATA, F., (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal*, Cizur Menor: Thomson Reuters Aranzadi, pp. 15-41.
- (2024), «Sistemas de gestión procesal, inteligencia artificial generativa y justicia orientada al dato: retos y desafíos», *Ius et scientia*, 10(2), pp. 11-32.
- COECKERLBERGH, M. (2021), *Ética de la inteligencia artificial*. Madrid: Cátedra.
- COLOMER HERNÁNDEZ, I. (2021), «Control y límites del uso de la información y los datos personales por parte de la inteligencia artificial en los procesos penales», en S. Barona Vilar (ed.), *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Valencia: Tirant lo Blanch, pp. 287-308.
- CORTINA ORTS, A. (2019), «Ética de la inteligencia artificial». *Anales de la Real Academia de Ciencias Morales y Políticas*, pp. 379-394.

- DELGADO MARTÍN, J. (2021), «Reflexiones sobre el estado actual de la transformación digital de la justicia». *Revista Acta Judicial*, 8, pp. 27-43.
- ETXEBERRÍA GURIDI, F. (2025), «La identificación biométrica remota “en diferido” en el Reglamento (UE) 2024/1689 de Inteligencia Artificial», *De la ejecución a la historia del derecho procesal y de sus protagonistas*, vol. 3. Barcelona: Atelier, pp. 201-228.
- FERREIRO BAAMONDE, X. (2024), «El Reglamento de Inteligencia Artificial y el proceso penal», en S. CALAZA LÓPEZ e I. ORDEÑANA GEZURAGA (dirs.), *Next Generation Justice: Digitalización e inteligencia artificial*, Madrid: La Ley, pp. 891-948.
- (2025), «No va sobre ética, va sobre democracia. El diseño algorítmico y la justicia penal», *De la ejecución a la historia del derecho procesal y de sus protagonistas*, vol. 3. Barcelona: Atelier, pp. 229-253.
- GLESS, S. (2020), «AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials», *Georgetown Journal of International Law*, vol. 51, pp. 195-254.
- GÓMEZ COLOMER, J. L. (2023a), *El juez robot. La independencia judicial en peligro*. Valencia: Tirant lo Blanch.
- (2023b), «Problemas legales del juez robot desde una perspectiva procesal y orgánica». *El proceso penal ante una nueva realidad tecnológica europea*, Cizur Menor: Thomson Reuters Aranzadi, pp. 163-193.
- JANSSEN, H. L. (2020), «An approach for a fundamental rights impact assessment to automated decision-making», *International Data Privacy Law*, vol. 10, pp. 76-106.
- KATSH, E., RABINOVICH-EINY, O. (2017), *Justicia digital: tecnología e internet de las disputas*. Oxford: Oxford University Press.
- KAUFMANN, M. (2018), «The co-construction of crime predictions. Dynamics between digital data, software and human beings», *Moral issues in intelligenceled policing*, N. R. FYFE, H. O. I. GUNDHUS y K. VRIST RONN (eds.), Abingdon: Routledge, pp. 143-160.
- MARTÍN DIZ, F. (2024a), «Derechos y garantías procesales penales fundamentales: una lectura en clave tecnológica». *Ius et scientia*, 10(1), pp. 52-81.
- (2024b), «Justicia Híbrida: La tecnología disruptiva al servicio del proceso». *Ius et veritas*, 68, pp. 113-129.
- PINEROS POLO, E. (2024), «El Juez-Robot y su encaje en la Constitución Española. La inteligencia artificial utilizada en el ámbito de la toma de decisiones por los tribunales». *Estudios de Deusto*, 72 (1), pp. 53-78.
- QUATTROCOLO, S. (2020), *Artificial Intelligence, Computational modelling and Criminal Proceedings. A framework for a European Legal Discussion*, Cham: Springer.
- SAN MIGUEL CASO, C. (2021), «La aplicación de la inteligencia artificial en el proceso: ¿un nuevo reto para las garantías procesales?». *Ius et scientia*, 1(7), pp. 286-303.
- SANCHIS CRESPO, C. (2023), «Inteligencia artificial y decisiones judiciales: crónica de una transformación anunciada». *Scire*, 29(2), pp. 65-84.
- SOURDIN, T. (2018), «Judge v Robot?: Artificial intelligence and judicial decision-making». *University of New South Wales Law Journal*, 41(4), pp. 1114-1133.

- TATA, C. (1998), «The Application of Judicial Intelligence and “Rules” to Systems Supporting Discretionary Judicial Decision-Making», *Artificial Intelligence and Law*, vol. 6, pp. 203-230.
- ZAVRSNIK, A. (2020), «Criminal Justice, artificial intelligence systems, and human rights», *ERA Forum*, 20, pp. 567-583.