



COMILLAS
UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

FACULTAD DE DERECHO

**LA IA Y LA PROPORCIONALIDAD EN LA
ADOPCIÓN DE MEDIDAS CAUTELARES
PERSONALES EN EL PROCESO PENAL**

Riesgo de sesgos en la predicción de reincidencia o fuga y su
compatibilidad con el art. 17 CE y la presunción de inocencia

Autor: Ángela Díaz de Santos

Tutor: Dra. Sara Díez Riaza

5º E-3 C

Área de Derecho Procesal

Madrid

Marzo 2026

ÍNDICE DE CONTENIDO

LISTADO DE ABREVIATURAS.....	4
INTRODUCCIÓN.....	5
1. JUSTIFICACIÓN DE INTERÉS Y OBJETIVOS PERSEGUIDOS.....	5
2. METODOLOGÍA Y PLAN DE TRABAJO.....	8
CAPÍTULO I. LAS MEDIDAS CAUTELARES PERSONALES EN EL PROCESO PENAL ESPAÑOL.....	10
1. PRESUPUESTOS PARA SU ADOPCIÓN.....	10
1.1. <i>Fumus boni iuris</i>	10
1.2. <i>Periculum in mora</i>	11
1.3. La integración de la IA.....	11
2. MARCO CONSTITUCIONAL.....	13
2.1. El derecho a la libertad.....	13
2.2. La presunción de inocencia.....	13
3. LA PROPORCIONALIDAD COMO CANON DE CONTROL.....	14
CAPÍTULO II. EL MARCO NORMATIVO EUROPEO DE IA EN LA EVALUACIÓN DEL RIESGO PROCESAL.....	16
1. REGLAMENTO DE IA: EL NUEVO PANORAMA EUROPEO.....	16
2. PROYECCIÓN EN EL SISTEMA ESPAÑOL.....	18
CAPÍTULO III. ANÁLISIS DE LA IRRUPCIÓN DE LA IA EN LA EVALUACIÓN DEL RIESGO PROCESAL.....	20
1. LOS <i>RISK ASSESSMENT TOOLS</i> O ALGORITMOS DE EVALUACIÓN DE RIESGO.....	21
1.1. Sistemas aplicados al <i>periculum in mora</i> en decisiones de libertad.....	21
1.1.1. <i>COMPAS</i> (Estados Unidos).....	21
1.1.2. <i>PSA</i> (Estados Unidos).....	24
1.1.3. <i>LSI-R</i> (Canadá).....	25

1.2.	Sistemas de predicción policial de riesgo delictivo	27
1.2.1.	<i>HART (Reino Unido)</i>	<i>27</i>
2.	PRECEDENTES EN EL ORDENAMIENTO JURIDÍDICO ESPAÑOL	28
2.1.	VioGén	28
2.2.	RisCanvi	30
2.3.	VeriPol	31
CAPÍTULO IV. LA IA ANTE EL MODELO ESPAÑOL DE JUSTICIA CAUTELAR.....		33
1.	TENSIONES ENTRE LAS GARANTÍAS PROCESALES Y LA <i>BLACK BOX</i> DE LOS SISTEMAS DE IA.....	33
1.1.	Transición a un derecho penal de autor	33
1.2.	Riesgo de indefensión	34
2.	SESGO DE AUTOMATIZACIÓN Y EXCLUSIVIDAD JURISDICCIONAL	35
3.	LA INSUFICIENCIA DE LA LECRIM: UN HORIZONTE DE REFORMA...	36
CONCLUSIONES		39
BIBLIOGRAFÍA		41
1.	LEGISLACIÓN.....	41
2.	JURISPRUDENCIA.....	42
3.	OBRAS DOCTRINALES	44
4.	RECURSOS DE INTERNET.....	47

LISTADO DE ABREVIATURAS

AESIA	Agencia Española de Supervisión de Inteligencia Artificial
Art./Arts.	Artículo/Artículos
CE	Constitución Española
<i>Cfr.</i>	<i>Confer</i> (idea extraída de la obra citada, pero no en sus exactos términos)
IA	Inteligencia Artificial
<i>Ibid.</i>	<i>Ibidem</i> (misma obra y distinta página que la cita anterior)
<i>Id.</i>	<i>Idem</i> (misma obra y página que la cita anterior)
LECrim	Ley de Enjuiciamiento Criminal
LOPJ	Ley Orgánica del Poder Judicial
<i>Op cit</i>	<i>Opere citato</i> (en una obra ya citada)
<i>RATs</i>	<i>Risk Assessment Tools</i>
RGPD	Reglamento General de Protección de Datos
RIA	Reglamento europeo de Inteligencia Artificial
Sistema COMPAS	<i>Correctional Offender Management Profiling for Alternative Sanctions</i>
Sistema HART	<i>Harm Assessment Risk Tool</i>
Sistema LSI-R	<i>Level of Service Inventory-Revised</i>
Sistema PSA	<i>Public Safety Assessment</i>
Sistema RisCanvi	<i>Risc i Canvi</i> (Riesgo y Cambio)
Sistema VeriPol	Sistema de Verificación Policial
Sistema VioGén	Sistema de Seguimiento Integral en los casos de Violencia de Género
TEDH	Tribunal Europeo de Derechos Humanos
TFG	Trabajo de Fin de Grado
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
<i>Vid.</i>	<i>Vide</i> (véase)

INTRODUCCIÓN

1. JUSTIFICACIÓN DE INTERÉS Y OBJETIVOS PERSEGUIDOS

Se atribuye al científico naturalista Charles Darwin la idea de que no es el más fuerte de las especies el que sobrevive, ni el más inteligente, sino el que mejor se adapta a los cambios. Y es que esta reflexión, formulada en el ámbito de la evolución biológica, encuentra hoy un eco evidente en la adaptación de los sistemas jurídicos a las transformaciones tecnológicas.

La Inteligencia Artificial (en adelante «IA») ha llegado para quedarse. Según García-Bernalt, cuando hablamos de IA «nos referimos a una noción centrada en la capacidad de elegir la mejor acción para lograr un determinado objetivo teniendo en consideración ciertos criterios que se deben optimizar en función de los recursos disponibles, siendo así la racionalidad una parte significativa de esta herramienta». La IA ha irrumpido en la sociedad y en los sistemas de administración de justicia de los Estados, proyectándose como un instrumento de mejora de la precisión, eficiencia y transparencia de los procedimientos¹.

Sin embargo, aún debe evaluarse la reacción del sistema jurídico español a los avances de la IA. En este caso, se focalizará en la adaptación del proceso penal. Sobre esta premisa, Manuel Marchena Gómez, magistrado de la Sala Segunda (de lo Penal) del Tribunal Supremo, ya en el año 2022 calificó el derecho codificado de nuestra jurisdicción penal como «insuficiente» para afrontar el impacto de las nuevas tecnologías: «el proceso penal no ha podido sustraerse al paso del tiempo»².

La Ley de Enjuiciamiento Criminal (en adelante «LECrim»)³, cuerpo normativo que desarrolla la actividad del procedimiento penal español, requiere de una actualización permanente para adaptarse a los potenciales desarrollos tecnológicos⁴. En línea con la

¹ Yáñez García-Bernalt, I., “La inteligencia artificial en el proceso penal: eficiencia versus garantías”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, p. 81 (<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.04>).

² Marchena Gómez, M., “Inteligencia artificial y jurisdicción penal”, *Real Academia de Doctores de España*, 2022, p. 7.

³ Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (Gaceta de Madrid nº 260, de 17 de septiembre de 1882).

⁴ Concepto del panorama jurídico actual que convive con la irrupción de la tecnología ilustrado en García Sánchez, M. D., “La necesidad de regulación de una nueva tipología cautelar frente a la delincuencia en el entorno digital”, *Crónica Jurídica Hispalense: revista de la Facultad de Derecho*, n. 22, 2024, p.180 (<https://hdl.handle.net/11441/175663>).

idea de adaptación al cambio de Darwin, el juez Marchena ya advirtió en su momento que «la renuncia generacional para sumarse a las posibilidades que ofrece la IA será también una renuncia a aprovecharse de las utilidades que ya están entre nosotros y que empiezan a vislumbrarse en un futuro no especialmente lejano»⁵. Es decir, quedarán rezagados aquellos sistemas que no se adapten a los cambios tecnológicos.

En todo caso, la adaptación del proceso penal español no puede comprenderse sin atender a las tensiones existentes en el sistema de medidas cautelares. La prisión provisional ha sido objeto de discusión doctrinal en innumerables ocasiones debido a su uso excesivo⁶, y en países como Estados Unidos, el porcentaje de población reclusa por habitante ha crecido exponencialmente en los últimos años, encareciendo el mantenimiento de los presos en todo el país⁷.

Con este panorama, no resulta extraño que en determinados ordenamientos jurídicos se haya impulsado la aplicación de algoritmos para auxiliar al juez en decisiones cautelares relacionadas con la privación de libertad u otras medidas restrictivas de derechos del procesado. Un ejemplo de ello es la herramienta COMPAS en EEUU, que «valora el riesgo de reincidencia del procesado y las necesidades criminológicas del sujeto»⁸ y que será objeto de análisis en capítulos posteriores.

La atención al Derecho comparado permite intuir la puesta en duda de la fiabilidad humana en la adopción de medidas cautelares personales. La decisión del juez puede verse condicionada por diversos sesgos «heurísticos y epistemológicos», es decir, por sus prejuicios, emociones, ideología, intuición, fatiga, anclaje o el recurso casi automático a recuerdos de casos anteriores⁹, lo que puede afectar a la apreciación del riesgo y poner en entredicho las garantías procesales del encausado.

Parte de la doctrina destaca que un diseño adecuado de un sistema de IA de evaluación

⁵ Marchena Gómez, M., *op. cit.*, p. 9.

⁶ Miranda, G., “Justicia algorítmica y medidas cautelares en el proceso penal. ¿Puede la IA solucionar los problemas de la decisión sobre la prisión provisional?”, *Castellarnau Penalistas*, 26 de septiembre de 2023 (disponible en <https://www.castellarnaupenalistas.com/>; última consulta 24/03/2026).

⁷ Muñoz Aranguren, A., “¿Derecho a una decisión humana? El uso de la inteligencia artificial en la predicción judicial de la reincidencia”, *Anuario Jurídico Secciones ICAM Sepin Colex*, 2021, p. 2.

⁸ Herramienta definida en Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., “Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos”, *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 1, 2022, pp. 281 y 282 (<https://doi.org/10.22197/rbdpp.v8i1.615>).

⁹ Dorado Ferrer, J., “Simón Castellano, Pere, Justicia cautelar e inteligencia artificial: La Alternativa a los atávicos heurísticos Judiciales, J. M. Bosch Editor, Barcelona, 2021, 260 pp., ISBN 978-84-123154-0-0”, *Estudios De Deusto*, vol. 69, n. 2, 2021, p. 350 ([https://doi.org/10.18543/ed-69\(2\)-2021pp347-352](https://doi.org/10.18543/ed-69(2)-2021pp347-352)).

de riesgo ayudaría a superar las deficiencias del modelo actual de medidas cautelares y a aportar objetividad al juez, que en ocasiones toma «improcedentemente» por analogía las mismas decisiones que en casos similares sin atender al caso concreto¹⁰.

Es fundamental en este punto analizar la otra cara de la moneda: los sesgos de la IA. Compañías como Amazon tuvieron que «abandonar» el uso de un algoritmo de IA encargado de filtrar perfiles en las fases preliminares de reclutamiento y selección de personal, debido a que la herramienta se inclinaba por el género masculino¹¹. No obstante, si en lugar de optar a un puesto de trabajo se optase por la libertad condicionada, el impacto sería muy diferente. Así, la adopción de algoritmos de IA de evaluación del riesgo de reincidencia o fuga como herramienta auxiliar en la decisión del juez podría caer en los mismos sesgos heurísticos que el ser humano¹².

Al sesgo humano y tecnológico se le suma la intervención del legislador europeo. La Unión Europea ha introducido un nuevo marco regulatorio a través del Reglamento de IA (en adelante «RIA»)¹³ que pone al ordenamiento jurídico español contra las cuerdas. La continuidad de los sistemas algorítmicos en el ámbito penal y policial está condicionada a obligaciones muy estrictas: el texto identifica como sistemas de IA «de alto riesgo» aquellos destinados a evaluar el riesgo de que una persona física cometa un delito o sea reincidente, así como los que detecten el estado emocional de las personas físicas (polígrafos)¹⁴.

La nueva normativa europea ha tenido un impacto notable en los ordenamientos jurídicos. En España, ha provocado la retirada de VeriPol, una herramienta de IA empleada por la Policía Nacional «capaz de detectar denuncias falsas de robo con violencia con una precisión de más del 90%», y cuyo uso se ha desestimado por la falta de información

¹⁰ Álvarez Buján, M. V., “Inteligencia artificial y medidas cautelares en el proceso penal: tutela judicial efectiva y autodeterminación informativa en potencial riesgo”, *Revista Española de Derecho Constitucional*, vol. 127, 2023, p. 196 (<https://doi.org/10.18042/cepc/redc.127.06>).

¹¹ Rubio, I., “Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres”, *El País*, 12 de octubre de 2018 (disponible en https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html; última consulta 24/03/2026).

¹² Dorado Ferrer, J., *op. cit.*, p. 351.

¹³ 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 y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 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) (DO L, 2024/1689, de 12 de julio de 2024) (DOUE 12 de julio de 2024).

¹⁴ *Vid.* apartados 6(b) y (d) del Anexo III del Reglamento (UE) de IA.

sobre su funcionamiento¹⁵.

La insuficiente transparencia y documentación de estos sistemas de IA «de alto riesgo» podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como el derecho a la defensa y a la presunción de inocencia (considerando 59).

Hoy, los sistemas de IA de predicción de reincidencia o fuga como herramienta de auxilio al juez son una nueva realidad a asimilar a fin de que, sin ser vinculantes sus resultados para el mismo, ayuden a lograr mejores resoluciones y a eliminar errores o injusticias¹⁶.

Pero ¿será capaz el proceso penal español de soportar los desafíos de la IA? ¿En qué condiciones se encuentra la LECrim para afrontar una adaptación integral de este tipo de sistemas en las decisiones cautelares? ¿Es momento de reformar los pilares del proceso penal en nuestro país y abrir paso a la innovación?

El objetivo de este Trabajo es analizar la posibilidad de crear un «ecosistema jurídico-tecnológico»¹⁷ en España que permita la inclusión de sistemas de IA de predicción de riesgo o reincidencia cuyo resultado sirva de apoyo al juez en la toma de decisiones de adopción de medidas cautelares personales.

2. METODOLOGÍA Y PLAN DE TRABAJO

Para abordar el objetivo planteado, el análisis sigue una metodología de investigación jurídica de carácter cualitativo y documental. Estas páginas realizan un estudio de la normativa, doctrina y jurisprudencia aplicables a las medidas cautelares personales en España y al uso de sistemas de IA en decisiones cautelares personales en el proceso penal. Para complementar este enfoque, se aporta la perspectiva del Derecho comparado, a fin de valorar críticamente el posible encaje de estos sistemas en el modelo español de justicia cautelar. Además, se ha recurrido de manera auxiliar a herramientas de IA generativa (como ChatGPT o Gemini) sólo en el contexto de las actividades descritas a continuación: para la corrección de estilo y lenguaje, la revisión formal del texto y la traducción puntual

¹⁵ García, T., Torrecillas, C., Maqueda, A., “La Policía Nacional deja de usar Veripol, su IA estrella para detectar denuncias falsas”, *El País*, 19 de marzo de 2025 (disponible en <https://elpais.com/tecnologia/2025-03-19/la-policia-nacional-deja-de-usar-veripol-su-ia-estrella-para-detectar-denuncias-falsas.html>; última consulta 24/03/2026).

¹⁶ *Cfr.* Álvarez Buján, M. V., *op. cit.*, pp. 204 y 205.

¹⁷ García Torres, M. L., “La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal”, *Ciencia Policial*, vol. 183, 2024, p. 107 (<https://doi.org/10.14201/cp.32177>).

de ciertos materiales.

En lo relativo al plan de trabajo, el presente Trabajo de Fin de Grado (en adelante, «TFG») se estructura en cuatro capítulos:

En primer lugar, el capítulo I lleva a cabo un análisis del sistema de medidas cautelares personales existente en el proceso penal español. Por un lado, se estudian los presupuestos necesarios para la adopción de decisiones cautelares personales, especialmente el *fumus boni iuris* y el *periculum in mora*: el objetivo es analizar el criterio más susceptible de ser evaluado por una herramienta de IA. Por otro lado, se aborda su encaje constitucional, en especial atención a los derechos fundamentales consagrados en los artículos 17 y 24.2 (relativos al derecho a la libertad y al derecho a la presunción de inocencia, respectivamente). Por último, el capítulo cierra con el análisis de la proporcionalidad como canon de control ante las decisiones cautelares.

En segundo lugar, el capítulo II trata el marco normativo europeo de la IA en la evaluación del riesgo procesal, para lo que se analiza el Reglamento de IA en lo relativo a los sistemas de IA alto riesgo objeto de este TFG. Posteriormente se valora la proyección normativa del RIA en el sistema jurídico español, así como su situación ante la posible entrada inminente de estos sistemas en el proceso penal.

En tercer lugar, el capítulo III analiza la irrupción de la IA en la evaluación del riesgo procesal a través del estudio de algunos de los sistemas algorítmicos existentes en otros ordenamientos jurídicos (EEUU, Canadá y Reino Unido) y en España, con el objetivo de identificar los riesgos para las garantías procesales del encausado. Para examinar sus consecuencias se ilustrarán además ciertos casos de uso relevantes.

Por último, el capítulo IV estudia la situación del proceso penal español para soportar la irrupción de estos sistemas de IA, y evalúa la necesidad o no de una reforma de la LECrim que adapte su contenido a la última tecnología.

CAPÍTULO I. LAS MEDIDAS CAUTELARES PERSONALES EN EL PROCESO PENAL ESPAÑOL

1. PRESUPUESTOS PARA SU ADOPCIÓN

Gómez Neira atribuye como finalidad de la regulación de las medidas cautelares la de garantizar «la efectividad del proceso, ya que comportan un real y efectivo aseguramiento de su desarrollo»¹⁸. En particular, las medidas cautelares personales tienen el objetivo de asegurar la presencia del investigado en el procedimiento, de evitar su entorpecimiento mediante la destrucción de la prueba¹⁹. La legitimación para adoptar este tipo de medidas restrictivas de derechos fundamentales se basa en la existencia de dos circunstancias esenciales: *fumus boni iuris* y *periculum in mora*²⁰.

1.1. *Fumus boni iuris*

En primer lugar, el *fumus boni iuris* o «apariencia de buen derecho» se concreta en el proceso penal en la atribución del hecho ilícito a la persona afectada por la medida cautelar, basado en indicios de criminalidad. El Tribunal Supremo (en adelante, «TS») ha definido este mínimo imprescindible para la adopción de la medida como un «juicio sobre la verosimilitud, racionalidad y fundamentación de los datos que apuntan hacia la responsabilidad penal de una determinada persona»²¹.

Este presupuesto comprende la existencia de ambos elementos objetivo y subjetivo. Por ejemplo, en el marco de la prisión provisional, el elemento objetivo requiere que existan hechos con apariencia delictiva y que estos lleven aparejada una pena privativa de libertad; y el elemento subjetivo implica la concurrencia de motivos suficientes para considerar responsable penalmente a la persona encausada²².

¹⁸ Borges Blázquez, R., “Algoritmización de la concesión de medidas cautelares en el proceso penal para la protección de víctimas de violencia de género. ¿Es capaz VIOGEN de interpretar el periculum in mora?”, *Actualidad Jurídica Iberoamericana*, n. 21, 2024, p. 386.

¹⁹ Definido en Redacción Lefebvre, “Medidas cautelares en el proceso penal”, *El Derecho*, 1 de septiembre de 2023 (disponible en <https://elderecho.com/medidas-cautelares-en-proceso-penal>; última consulta 24/03/2026).

²⁰ *Vid.* Fundamento Jurídico Primero de la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 159/1996, de 24 de febrero de 1996 [versión electrónica – base de datos Cendoj. Roj: STS 1172/1996; ECLI:ES:TS:1996:1172]. Fecha de la última consulta: 24 de marzo de 2026.

²¹ *Vid.* Fundamento Jurídico Segundo de la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 578/2012, de 26 de junio de 2012 [versión electrónica – base de datos Cendoj. Roj: STS 5698/2012; ECLI:ES:TS:2012:5698]. Fecha de la última consulta: 24 de marzo de 2026.

²² Álvarez Buján, M. V., *op. cit.*, pp. 198 y 199.

1.2. *Periculum in mora*

En segundo lugar, el *periculum in mora* o «peligro de mora procesal» introduce la necesidad del juez de justificar la medida cautelar personal por el riesgo irreparable que puede generar su falta de adopción²³. Estos riesgos se identifican con (i) asegurar la presencia del investigado en el proceso, es decir, evitar el riesgo de fuga, (ii) evitar la ocultación, manipulación o destrucción de fuentes de prueba, o (iii) impedir la reiteración delictiva (art. 503.1.3º LECrim). Son los presupuestos que legitiman la adopción de «cualquier medida cautelar restrictiva de la libertad personal»²⁴.

Además, tanto la LECrim como el TS han definido los datos orientativos que deben ser valorados de manera conjunta en el análisis del riesgo de fuga²⁵. Estos son «la naturaleza del hecho, la gravedad de la pena que pudiera imponerse al imputado, la situación familiar, laboral y económica de éste, así como la inminencia de la celebración del juicio oral»²⁶.

1.3. La integración de la IA

Una vez definidos los presupuestos necesarios en la adopción de medidas cautelares personales, procede delimitar el contexto en el que la IA va a intervenir.

Autores como Neira Pena han analizado la posible intervención de la IA en la determinación del *fumus boni iuris*, pero terminan rechazándola. El ejercicio de imputación del delito al individuo implica «reconstruir el pasado, valorando jurídicamente los hechos investigados», por lo que la IA «difícilmente puede sustituir al juicio jurisdiccional»²⁷.

Sin embargo, el criterio del *periculum in mora* sí implica «predecir el futuro» y «asignar probabilidades a hechos inciertos»²⁸, ya que se basa en el cálculo de probabilidades de comportamientos futuros (riesgos). Así, el *periculum in mora* resulta ser el presupuesto más susceptible de ser determinado por un sistema de IA predictiva, al ser el más

²³ García Sánchez, M. D., *op. cit.*, p. 188.

²⁴ Marchena Gómez, M., *op. cit.*, p. 53.

²⁵ Neira Pena, A. M., “Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional”, *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 3, 2021, p. 1910 (<https://doi.org/10.22197/rbdpp.v7i3.618>).

²⁶ Auto del Tribunal Supremo (Sala de lo Penal, Sección 1ª), rec. 20907/2017, de 18 de junio de 2018 [versión electrónica – base de datos Cendoj. Roj: ATS 6831/2018; ECLI:ES:TS:2018:6831A]. Fecha de la última consulta: 24 de marzo de 2026.

²⁷ Neira Pena, A. M., *op. cit.*, p. 1908.

²⁸ *Id.*

objetivable de los dos, ya que no implica un juicio de valor sobre la conducta humana como ocurre en la determinación del *fumus boni iuris*²⁹.

En línea con esta idea, Sánchez Sáez defiende que, aunque la potestad de ponderar los intereses en conflicto corresponde en exclusiva al juez, la IA puede aportar un soporte técnico en la evaluación de riesgos científicos o técnicos que amenacen el objeto del proceso. Sáez ilustra esta reflexión comparando los riesgos del proceso penal con los del ámbito contencioso-administrativo, como el porcentaje de probabilidad de derrumbe de una casa o la evaluación del estado de conservación de las obras públicas. En este ámbito, un sistema de IA aporta porcentajes de probabilidad que auxilian la labor del juez y Sáez afirma su utilidad para evaluar la reincidencia del individuo en el proceso penal³⁰.

Por último, la jurisprudencia se ha pronunciado en este sentido acerca del margen de subjetividad del juez en la predicción del riesgo ante la imposición de medidas cautelares³¹. El TS aborda la necesidad de superar las «meras hipótesis subjetivas» o la simple convicción del juzgador en la adopción de medidas restrictivas de derechos³². Para ello, exige que la decisión cautelar descansa sobre «datos objetivos» que proporcionen una base real de la que pueda inferirse el riesgo, rechazando que estos indicios consistan en meras «valoraciones acerca de la persona»³³.

Por ello, introducir un sistema de IA que auxilie al juez en la valoración del *periculum* ayudaría a mitigar el riesgo de adoptar una decisión cautelar basada en meras impresiones.

²⁹ Cfr. Borges Blázquez, R., *op cit*, p. 392; Neira Pena, A. M., *op cit*, p. 1908.

³⁰ Sánchez Sáez, A. J., “El posible uso de la inteligencia artificial en el ámbito judicial: contexto jurídico español y europeo. Especial referencia al contencioso-administrativo”, *Rivista italiana di informatica e diritto*, vol. 5, n. 2, 2023, p. 191 (<https://doi.org/10.32091/RIID0118>).

³¹ Dorado Ferrer, J., *op cit*, p. 349.

³² Vid. Fundamento Jurídico Cuarto de la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 580/2021, de 1 de julio de 2021 [versión electrónica – base de datos Cendoj. Roj: STS 2834/2021; ECLI:ES:TS:2021:2834]. Fecha de la última consulta: 24 de marzo de 2026.

³³ Vid. Fundamento Jurídico nº 12 de la Sentencia del Tribunal Constitucional (Pleno) núm. 184/2003, de 23 de octubre de 2003 [versión electrónica – BOE. Ref: BOE-T-2003-20770]. Fecha de la última consulta: 24 de marzo de 2026.

2. MARCO CONSTITUCIONAL

Al carecer de características humanas esenciales, si la decisión cautelar se fundamenta en un resultado de IA no transparente, puede poner en entredicho la imparcialidad del juez y el derecho de defensa del encausado. La elección de este marco normativo se debe a que ambos arts. 17 y 24.2 de la Constitución Española (en adelante, «CE»)³⁴ inducen a interpretar que el uso de la IA sea un complemento auxiliar del magistrado, y no un sustituto de la decisión humana.

2.1. El derecho a la libertad

La elección del artículo 17 CE como primer pilar de este análisis responde a la injerencia radical del Estado en la esfera del individuo que supone la imposición de una medida cautelar personal: la privación del derecho fundamental a la libertad y a la seguridad. El precepto establece que «toda persona tiene derecho a la libertad y a la seguridad» y continúa afirmando que nadie puede ser privado de ella «sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley»³⁵.

Desde esta perspectiva, la incorporación de sistemas de IA como herramienta auxiliar en la imposición de medidas cautelares personales debe someterse a un control judicial reforzado al tratarse de limitaciones de la libertad previas a una condena firme. En este contexto, es fundamental que el juez conozca el proceso intelectual seguido por el algoritmo y revise críticamente sus resultados, con el fin de impedir la vulneración de los denominados «derechos procesales fundamentales»³⁶ por una implantación irreflexiva de estas tecnologías³⁷.

2.2. La presunción de inocencia

Por su parte y de forma complementaria, el principio de presunción de inocencia del sospechoso o investigado previsto en el artículo 24.2 de la Carta Magna constituye un pilar fundamental del proceso penal en la formulación del juicio sobre la culpabilidad o inocencia, ya que obliga a tratar al investigado como inocente hasta que una sentencia

³⁴ Constitución Española. Boletín Oficial del Estado nº 311, de 29 de diciembre de 1978.

³⁵ Artículo 17.1 de la Constitución Española.

³⁶ Concepto definido por Sánchez Sáez, A. J., *op cit*, p. 177, entre los que incluye «la igualdad, la intimidad o privacidad, a un juicio justo, tutela judicial efectiva, juez imparcial, presunción de inocencia, proporcionalidad, etc.».

³⁷ Sánchez Sáez, A. J., *op cit*, p. 177.

firme declare lo contrario³⁸.

El uso de sistemas de IA predictiva para el objeto de estudio del presente TFG podría comprometer la garantía del derecho a la presunción de inocencia del individuo. Como desarrolla Yáñez, «la naturaleza de la IA y las decisiones basadas en patrones y estadísticas pueden predisponer a las autoridades a percibir, incorrectamente, a individuos como culpables o peligrosos incluso sin pruebas concluyentes que permitan desvirtuar la citada presunción». Es decir, la utilización de este tipo de algoritmos, cuyo sistema se basa en datos históricos, conlleva el riesgo de que funcione como una herramienta de «pre-criminalización» del sujeto³⁹.

3. LA PROPORCIONALIDAD COMO CANON DE CONTROL

A su vez, cualquier restricción de la libertad debe cumplir el principio de proporcionalidad. La jurisprudencia del TS establece que la vigencia de la proporcionalidad «aunque no está expresamente reconocida en la Constitución Española, no admite dudas (...) tal principio es el “... eje definidor siempre de cualquier decisión judicial⁴⁰...”, (...) que debe venir dictada por la ponderación entre los bienes en conflicto. Dentro del sistema de justicia penal, la pena viene a ser la justa respuesta a la gravedad del hecho enjuiciado y al nivel de culpabilidad de su autor»⁴¹.

El requisito de la proporcionalidad de la pena impuesta se aplicará de la misma manera a la imposición de la medida cautelar. Además de la triple exigencia que legitima el principio de proporcionalidad (necesidad o subsidiariedad de la medida, idoneidad y proporcionalidad en sentido estricto)⁴², la doctrina alude a la inclusión de controles que aseguren el cumplimiento de la proporcionalidad en el uso de sistemas de IA predictiva

³⁸ Yáñez García-Bernalt, I., *op. cit.*, p. 93.

³⁹ *Ibid.*, p. 94.

⁴⁰ *Vid.* Fundamento Jurídico Cuarto de la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 845/1998, de 18 de junio de 1998 [versión electrónica – base de datos Cendoj. Roj: STS 4049/1998; ECLI:ES:TS:1998:4049]. Fecha de la última consulta: 24 de marzo de 2026.

⁴¹ *Vid.* Fundamento Jurídico Segundo del Auto del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 1252/2021, de 25 de noviembre de 2021 [versión electrónica – base de datos Cendoj. Roj: ATS 16740/2021; ECLI:ES:TS:2021:16740A]. Fecha de la última consulta: 24 de marzo de 2026.

⁴² Para que una medida cautelar sea legítima debe cumplir con una triple exigencia: **juicio de idoneidad**, es decir, que sea apta para satisfacer el objetivo propuesto (como el riesgo de fuga); **juicio de necesidad**, en el sentido de que no exista otra medida más moderada que logre el mismo objetivo; y **juicio de proporcionalidad en sentido estricto**, que implica que una vez haya sido ponderada, su beneficio para el interés general debe ser mayor al perjuicio que genere sobre los valores en conflicto. (*Cfr.* Sentencia del Tribunal Constitucional (Sala Primera) núm. 207/1996, de 16 de diciembre de 1996 [versión electrónica – BOE. Ref: BOE-T-1997-1175]. Fecha de la última consulta: 24 de marzo de 2026. Fundamento jurídico Cuarto, apartado E).

en el proceso penal. Estos controles deberían asegurar, en primer lugar, la supervisión de la legalidad del algoritmo de IA y el tratamiento de los datos empleados; en segundo lugar, la preservación de la ineludible intervención humana de quien encarne el órgano judicial competente a la hora de adoptar la decisión; y, por último, la transparencia del sistema IA para no incurrir en sesgos⁴³.

Con esta premisa, si la proporcionalidad actúa como canon material de legitimidad y los controles de legalidad, intervención humana y transparencia operan como garantía frente al riesgo de los sistemas de IA, resulta necesario analizar a continuación cómo estas exigencias han sido recogidas y desarrolladas por el legislador europeo.

⁴³ Álvarez Buján, M. V., *op cit*, p. 203.

CAPÍTULO II. EL MARCO NORMATIVO EUROPEO DE IA EN LA EVALUACIÓN DEL RIESGO PROCESAL

Una vez asentado el escenario normativo de las medidas cautelares personales en el proceso penal español (que responde a cómo debe enjuiciarse la restricción de libertad), habrá que atender al marco europeo para analizar los requisitos que deben cumplir los sistemas de IA que quieran intervenir en esa decisión cautelar para auxiliar al juez, y servirle de apoyo en la valoración del riesgo.

En este capítulo se analizan las principales exigencias impuestas por la Unión Europea para este tipo de sistemas y su proyección sobre el ordenamiento español, así como la situación normativa en la que se encuentra para asumir la entrada inminente de este tipo de sistemas de IA en el proceso penal.

1. REGLAMENTO DE IA: EL NUEVO PANORAMA EUROPEO

El Reglamento europeo de IA somete a determinados sistemas de IA utilizados en contextos sensibles a un control reforzado. Entre estos sistemas calificados como «de alto riesgo», se incluyen los siguientes:

«d) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para **evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito** atendiendo no solo a la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos»⁴⁴.

En este sentido, el considerando 42 asegura la preservación del derecho a la presunción de inocencia en el uso de este tipo de sistemas de IA. Para ello, el Reglamento prohíbe los sistemas de predicción de riesgo que se basen únicamente en «la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad»⁴⁵. Esto implica que las personas físicas deben ser juzgadas por su

⁴⁴ Vid. apartado 6(d) del Anexo III del Reglamento (UE) de IA: “Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA **que formen parte de cualquiera de los ámbitos siguientes**: (...) 6. **Garantía del cumplimiento del Derecho**, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable: (...) d) Sistemas de IA destinados a...”.

⁴⁵ Vid. considerando 42 del Reglamento (UE) de IA: “En consonancia con la presunción de inocencia (...)”

comportamiento real y nunca a partir de comportamientos que haya predicho una IA basándose únicamente en perfiles o rasgos de la personalidad⁴⁶.

Para que el despliegue de estos sistemas se realice conforme a la normativa europea, el texto establece una serie de obligaciones. Algunas de las más relevantes para los sistemas de IA analizados en el presente Trabajo son, entre otras: por un lado, evitar el «sesgo de automatización», definido como la tendencia humana a confiar en exceso en los resultados de la máquina al tomar decisiones críticas⁴⁷. Por ello, el uso del sistema debe ser supervisado por personas físicas. Parte de la doctrina comparte la preocupación de que, si los jueces aceptan y aplican la decisión de la máquina sin cuestionarla, la decisión se vuelve totalmente automatizada⁴⁸.

Es importante en este contexto hacer referencia al Reglamento europeo General de Protección de Datos (RGPD)⁴⁹. El RGPD establece una prohibición general a las decisiones automatizadas en su artículo 22.1: «todo interesado tendrá derecho 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»⁵⁰.

En esta línea, el Tribunal de Justicia de la Unión Europea (TJUE) ha trasladado su preocupación por el sesgo de automatización en casos como *SCHUFA Holding*⁵¹. El algoritmo de la empresa alemana emitía, a través de la recopilación de datos personales, una puntuación o *scoring* crediticio para evaluar la solvencia o el riesgo de impago de un

las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en (...) características de su personalidad, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo, **sin una valoración humana** y sin que exista una sospecha razonable, **basada en hechos objetivos comprobables**, de que dicha persona está implicada en una actividad delictiva (...)

⁴⁶ Cfr. apartado 1(d) del art. 5 del Reglamento (UE) de IA sobre “Prácticas de IA prohibidas”.

⁴⁷ Vid. apartado 4(c) del art. 14 del Reglamento (UE) de IA sobre “Supervisión humana” como requisito de los sistemas de IA de alto riesgo.

⁴⁸ Ensel, L., “Las sentencias algorítmicas frente al principio de culpabilidad y el derecho a ser oído en el proceso” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, p. 246.

⁴⁹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE 4 de mayo de 2016).

⁵⁰ Vid. art. 22 RGPD sobre las “Decisiones individuales automatizadas, incluida la elaboración de perfiles”.

⁵¹ Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), asunto C-634/21, *SCHUFA Holding (Scoring)*, de 7 de diciembre de 2023 [versión electrónica – EUR-Lex. ECLI:EU:C:2023:957]. Fecha de la última consulta: 24 de marzo de 2026.

individuo, puntuación que podía ser muy condicionante de la decisión posterior de un tercero. Así, el TJUE sentenció en diciembre de 2023 que la generación de un valor de probabilidad por un algoritmo deriva en una decisión automatizada cuando un tercero basa en ella su resolución de manera «determinante»⁵². Trasladado al juicio penal, si un juez aceptase el nivel de riesgo emitido por el sistema de IA sin una evaluación crítica del sujeto, se estaría produciendo una «laguna en la protección jurídica» del individuo⁵³ lo que omite la intervención humana que exige el Reglamento de IA.

Por otro lado, regula la obligación de asegurar que los datos suministrados al sistema «carecerán de errores»⁵⁴ para evitar el sesgo de la IA. El magistrado Marchena Gómez advierte de la presencia de un riesgo real de que el propio diseño del algoritmo esté «descompensado en beneficio de una clase, de un conjunto de sujetos o de unos intereses predominantes» por el uso de datos sesgados⁵⁵.

Además, el sistema debe asegurar la trazabilidad y la transparencia, que implica que toda persona afectada tiene derecho a obtener una explicación clara sobre el papel que la IA ha tenido en el proceso de toma de decisiones que afecten a sus derechos fundamentales (considerando 171).

2. PROYECCIÓN EN EL SISTEMA ESPAÑOL

Las obligaciones establecidas por el Reglamento europeo de IA para los sistemas de evaluación de riesgo delictivo (incluidos en los sistemas de IA de alto riesgo del anexo III del RIA) comenzarán a ser exigibles el 2 de agosto de 2026⁵⁶. Antes de la plena aplicación del Reglamento de IA, el sistema español ya cuenta con una base normativa frente a la irrupción de la tecnología en el proceso penal.

Entre los precedentes normativos, la Ley Orgánica 7/2021 (que traspone la Directiva 2016/680)⁵⁷, y la Ley Orgánica 3/2018 (adaptación a la legislación española del RGPD)⁵⁸,

⁵² *Idem.*, véase el fallo de la sentencia.

⁵³ *Idem.*, véase la cuestión prejudicial nº 23.

⁵⁴ *Vid.* apartado 3 del art. 10 del Reglamento (UE) de IA sobre “Datos y gobernanza de datos” como requisito de los sistemas de IA de alto riesgo.

⁵⁵ Marchena Gómez, M., *op. cit.*, p. 49.

⁵⁶ *Vid.* art. 113 RIA sobre la entrada en vigor y aplicación.

⁵⁷ Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE 27 de mayo de 2021).

⁵⁸ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

ofrecen una protección directa frente a la opacidad del algoritmo y a las decisiones automatizadas: se prohíben las decisiones basadas únicamente en un tratamiento automatizado que produzcan efectos jurídicos negativos para el investigado⁵⁹.

La implementación más reciente de esta tecnología (IA) se encuentra en el Real Decreto-ley 6/2023⁶⁰, que impulsa la digitalización de la justicia en España, y regula las «actuaciones asistidas» por IA. Su art. 57 define estas actuaciones como borradores generados por sistemas de IA a modo de apoyo, pero subraya que «en ningún caso el borrador documental así generado constituirá por sí una resolución judicial o procesal, sin validación de la autoridad competente». Es decir, en el supuesto actual de sistemas de IA predictivos de riesgo, sólo el juez podría dar validez final a su aplicabilidad en la decisión de medidas cautelares, evitando así la «deshumanización de la justicia»⁶¹.

Además, España ha creado las instituciones necesarias para cumplir las exigencias de la UE. En 2023 aprobó el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA)⁶², designando con ello la autoridad nacional responsable de controlar la aplicación del Reglamento de IA. Y, por otro lado, el Real Decreto 817/2023⁶³ creó «el primer entorno controlado de pruebas o *sandbox*» para experimentar el impacto de la implementación de los requisitos exigidos a los sistemas de IA de alto riesgo⁶⁴.

De esta manera, con la adopción de ambas medidas, España ha anticipado el cumplimiento de la obligación europea de designar autoridades de vigilancia y control (considerando 153 RIA).

Una vez sentado el marco normativo europeo y nacional sobre los sistemas de IA de alto riesgo, es preciso estudiar a continuación los sistemas de prevención de riesgo que existen en las jurisdicciones de Derecho comparado y en la española, a la vista de comprobar su encaje legal y sus defectos para prevenir errores en el futuro.

⁵⁹ Cuatrecasas Monforte, C., *op cit*, p. 283.

⁶⁰ Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (BOE 20 de diciembre de 2023).

⁶¹ Ese riesgo de deshumanización existe como consecuencia de «ir delegando sin darnos cuenta cada vez más funciones en la IA», como se analiza en Bueno de Mata, F., “Sistemas de gestión procesal, inteligencia artificial generativa y justicia orientada al dato: retos y desafíos”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, p. 21 (<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.01>).

⁶² Para más información *vid.* página web oficial de AESIA (<https://aesia.digital.gob.es/es>).

⁶³ Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (BOE 9 de noviembre de 2023).

⁶⁴ Bueno de Mata, F., *op cit.*, pp. 27 y 28.

CAPÍTULO III. ANÁLISIS DE LA IRRUPCIÓN DE LA IA EN LA EVALUACIÓN DEL RIESGO PROCESAL

Este capítulo analiza el estado de la cuestión mediante el estudio de algunas de las herramientas existentes tanto en las diferentes jurisdicciones como en el ordenamiento jurídico español, en orden de mayor aplicabilidad funcional a las decisiones sobre medidas cautelares. Es decir, se analizan primero aquellas que más se asemejen a un algoritmo de apoyo al juez en decisiones cautelares (o que lo sean propiamente), y se continúa con ciertos sistemas predictivos con características similares existentes en la justicia penal española cuya observancia puede ser de gran utilidad.

En primer lugar, se aborda el concepto de los algoritmos de evaluación de riesgo (conocidos como *risk assessment tools*) mediante la ilustración de casos de uso relevantes en EEUU, Canadá y Reino Unido, y, en segundo lugar, los precedentes de justicia penal predictiva existentes en España.

Aunque la doctrina suele incluir las herramientas analizadas a continuación dentro del fenómeno amplio de la denominada «justicia penal predictiva»⁶⁵, desde un punto de vista técnico estos sistemas de IA no lo son en sentido estricto⁶⁶. No obstante, su capacidad para predecir el comportamiento futuro de los individuos de manera automática y su apoyo al juez en la toma de decisiones, justifican su inclusión en el estudio acerca del impacto de los algoritmos predictivos en el proceso penal. Por tanto, todos los sistemas analizados a continuación se engloban en el concepto de «justicia penal predictiva»⁶⁷.

El objetivo del análisis comparado es reconocer las flaquezas de estos sistemas (que ya se han detectado en la práctica) para determinar el impacto que supondría la implantación en España de un sistema de IA predictiva de decisiones cautelares sobre los derechos fundamentales del proceso, más concretamente sobre los arts. 17 y 24.2 CE y su compatibilidad con el principio de proporcionalidad y con los estándares europeos sobre los sistemas de IA de alto riesgo.

⁶⁵ García Torres, M. L., *op cit*, pp. 91 y 115.

⁶⁶ Gimeno Beviá, J., “Policía y justicia predictiva en España: análisis actual y reflexión crítica” en De Luca, J. A, Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, p. 151.

⁶⁷ Definida en García Torres, M. L., *op cit*, p. 117 como «el conjunto de herramientas que buscan la eficiencia procesal, que supone una mejora en la calidad de la toma de decisiones y una aminoración del trabajo realizado por los jueces».

1. LOS *RISK ASSESSMENT TOOLS* O ALGORITMOS DE EVALUACIÓN DE RIESGO

En la actualidad, existen algoritmos de predicción de riesgo conocidos como *Risk Assessment Tools (RATs)*, que en países como Estados Unidos superan las 150 modalidades empleadas en más de 20 estados⁶⁸. Como punto de partida, se analizan en este bloque algunos de los diferentes sistemas diseñados para asistir al juez en las decisiones sobre la situación personal del individuo en todas las fases del juicio penal y con posterioridad a este⁶⁹.

A continuación, se exponen los sistemas más resonados de las diferentes jurisdicciones con la ilustración de algunos casos de uso para valorar su impacto: por un lado (i) los sistemas aplicados en la determinación del *periculum in mora* para la imposición de restricciones de la libertad, como por ejemplo la probabilidad de reincidencia delictiva o de incomparecencia ante el tribunal (como se ilustró anteriormente, entre los presupuestos necesarios para la adopción de medidas cautelares: *fumus boni iuris* y el *periculum in mora*, el segundo es el más susceptible de ser determinado por un sistema de IA predictiva, al ser el más objetivable de los dos); y, por otro lado (ii) un ejemplo de sistema de predicción policial de riesgo delictivo.

1.1. Sistemas aplicados al *periculum in mora* en decisiones de libertad

1.1.1. COMPAS (Estados Unidos)

El sistema COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) es «un software informático que ayuda a los jueces a tomar la decisión del ingreso en un centro penitenciario o mantenimiento de la libertad en función de la probabilidad de reincidencia del investigado»⁷⁰. Se considera el algoritmo de evaluación de riesgos más extendido del sistema penal de Estados Unidos.

Impulsado en 1998 por la empresa privada estadounidense Northpointe, este sistema de apoyo a la decisión del juez estima la probabilidad de reincidencia y orienta, en

⁶⁸ Álvarez Buján, M. V., *op cit*, p. 197.

⁶⁹ Cuatrecasas Monforte, C., “La Inteligencia Artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos”, Universitat Ramon Llull, 2022, p. 273 (disponible en <http://hdl.handle.net/10803/675100>; última consulta 24/03/2026).

⁷⁰ Calaza López, S., “Transición digital de la justicia” en Llorente Sánchez-Arjona, M., Calaza López, S. (dirs.), Muínelo Cobo, J. C. (coord.), *Digitalización de la justicia: Prevención, Investigación y Enjuiciamiento*, Thomson Reuters-Aranzadi, Pamplona, 2022, p. 45.

consecuencia, el grado de supervisión, intervención o tratamiento sugerido respecto del acusado o penado⁷¹. La herramienta emite una puntuación de riesgo (del 1 al 10) asociado al individuo tras procesar su historial de antecedentes penales junto con las respuestas de los individuos a un cuestionario de 137 preguntas que evalúan las siguientes categorías: la participación delictiva, las relaciones y estilo de vida, la personalidad y actitudes, la familia y la exclusión social⁷².

Para conocer su implicación y su afectación a los derechos fundamentales del proceso es preciso hacer referencia a un caso de uso de gran relevancia. El caso *Wisconsin State vs. Loomis*⁷³ (2016) supone el segundo pronunciamiento de un tribunal en la historia sobre «la admisibilidad del uso de herramientas IA dentro del proceso penal»⁷⁴. El primer pronunciamiento fue el de la Corte Suprema de Indiana en 2010 por el caso *Malenchik vs. State of Indiana*⁷⁵, en referencia a la admisibilidad del algoritmo LSI-R, que será analizado más adelante en el presente capítulo.

En el asunto *State vs. Loomis*, Eric Loomis fue condenado a seis años de prisión y cinco años de libertad vigilada tras ser vinculado a un tiroteo. El juez de instancia justificó la severidad de la pena, entre otros, mediante un informe de la Fiscalía que aportaba una evaluación de riesgo de COMPAS basada en sus antecedentes y que asignaba a Loomis un «riesgo extremadamente alto» de reincidencia⁷⁶.

La defensa recurrió alegando que se había vulnerado su derecho al debido proceso por, entre otros, la violación del derecho «a ser juzgado en base a información precisa»⁷⁷. Argumentaron que el uso de un algoritmo amparado por el secreto comercial impide que el acusado pueda revisar, cuestionar o refutar la validez del cálculo de riesgo que condicionaba su libertad. Es decir, que la falta de transparencia del algoritmo había tenido una consecuencia muy perjudicial sobre sus derechos procesales fundamentales⁷⁸.

⁷¹ Cuatrecasas Monforte, C., *op cit*, p. 260.

⁷² *Ibid.*, p. 273.

⁷³ Sentencia de la Corte Suprema de Wisconsin, *State v. Loomis*, núm. 2015AP157-CR, de 13 de julio de 2016, [versión electrónica – base de datos vLex. Ref: 371 Wis.2d 235, 881 N.W.2d 749 (Wis. 2016)] (disponible en <https://case-law.vlex.com/vid/state-v-loomis-no-888404547>). Fecha de la última consulta: 24 de marzo de 2026.

⁷⁴ Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., *op cit*, p. 287.

⁷⁵ Martínez Garay, L., “Peligrosidad, algoritmos y due process: el caso *State v. Loomis*”, *Revista de Derecho Penal y Criminología*, n. 20, 3ª época, 2020, p. 494 (<https://doi.org/10.5944/rdpc.20.2018.26484>).

⁷⁶ Martínez Garay, L., “Peligrosidad, algoritmos y due process...”, *op cit*, p. 490.

⁷⁷ Traducido del término empleado en la Sentencia de la Corte Suprema de Wisconsin, *State v. Loomis*, núm. 2015AP157-CR...: «*to be sentenced upon accurate information*».

⁷⁸ *Vid.* nota al pie nº 36 para profundizar el concepto «derechos procesales fundamentales».

La Corte Suprema de Wisconsin rechazó el recurso, entre otros motivos, al considerar que el acusado sí «tuvo oportunidad de verificar que dichos datos eran correctos»⁷⁹ y que «el uso correcto de un sistema de evaluación del riesgo no conlleva, por sí solo, una vulneración del derecho al debido proceso»⁸⁰. Sin embargo, sentenció que todo uso futuro del informe COMPAS de evaluación de riesgos debía incluir advertencias sobre su opacidad y sus limitaciones técnicas.

Entre esas limitaciones, el Tribunal citó el estudio de ProPublica, un análisis de los resultados de COMPAS en más de 7.000 casos en Florida que evidenció que el algoritmo era racista. Según el estudio, los acusados negros tenían el doble de probabilidades de ser clasificados como «de riesgo alto» (*rated high risk*) en comparación con los blancos (44,9% vs. 23,5%), que eran calificados «de riesgo bajo» (*rated low risk*) a pesar de reincidir⁸¹.

El análisis de este caso de uso ha permitido identificar varias flaquezas del algoritmo en la práctica. Por un lado, el sesgo de la IA como amenaza a la neutralidad de los sistemas jurídicos, ya que la herramienta se nutre a base de «sesgos sistémicos» presentes en la recopilación de antecedentes penales que procesa la herramienta⁸².

Y, por otro lado, el concepto «caja negra» o *black box* al que hace referencia la Corte Suprema de Wisconsin con la necesidad de alertar de la opacidad del algoritmo. Este término implica que «el proceso de “toma de decisiones” (del sistema de IA) es complejo y generalmente se asemeja al de una “caja negra” dentro de la cual no se puede conocer cómo ocurren las cosas»⁸³.

⁷⁹ Martínez Garay, L., “Peligrosidad, algoritmos y due process...”, *op cit*, p. 491.

⁸⁰ Marchena Gómez, M., *op. cit*, p. 54.

⁸¹ Angwin, J., Larson, J., Mattu, S., Kirchner, L., “Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks”, *ProPublica*, 23 de mayo de 2016 (disponible en <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; última consulta 24/03/2026).

⁸² Martínez Garay, L., “Peligrosidad, algoritmos y due process...”, *op cit*, p. 497 aborda el concepto de «sesgo sistémico» propio de los algoritmos predictivos de la justicia penal, y sostiene que «incorporan, perpetúan y exacerbaban las discriminaciones estructurales del sistema en el que actúan y del que se alimentan».

⁸³ De Luca, J. A., “Prólogo e introducción” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, p. 10.

1.1.2. PSA (Estados Unidos)

Desarrollada en 2013 por la fundación Arnold Ventures, la herramienta PSA (*Public Safety Assessment*) surgió con el objetivo de erradicar los sesgos racistas y corregir la opacidad de sistemas como COMPAS a través de la transparencia y objetividad⁸⁴.

Es una herramienta cuyos factores de ponderación son públicos (no hay secreto comercial como ocurría con COMPAS) y, a diferencia de otros modelos, el algoritmo PSA prescinde de entrevistas personales y se basa en 9 factores objetivos como la edad del investigado en el momento de la detención o el historial de incomparecencias previas. En función de ello, la herramienta está diseñada para predecir tres resultados en la etapa previa al juicio (*pretrial stage*): la probabilidad de incomparecencia en el juicio (*Failure to Appear – FTA*), el riesgo de nueva actividad criminal o reincidencia (*New Criminal Arrest – NCA*) y un indicador específico de nuevo arresto por delito violento (*New Violent Criminal Arrest – NVCA*).

El fin del sistema PSA es objetivar el riesgo procesal basándose en datos administrativos (edad, antecedentes penales, etc.) y dar recomendaciones al juez. Busca «maximizar la comparecencia previa al juicio» y garantizar la seguridad minimizando la reincidencia⁸⁵.

En Nueva Jersey, su implantación formó parte de la *Criminal Justice Reform* que entró en vigor en 2017. Uno de los objetivos de la Reforma era sustituir el sistema de fianzas (el pago a cambio de ser liberado de la prisión preventiva tras la detención) por otro basado en el riesgo del individuo, para evitar que la privación de libertad dependiera de la capacidad económica del acusado. Un estudio realizado en 2019 argumentó que «antes de la reforma, el 12% de las personas recluidas en las cárceles de Nueva Jersey permanecían allí únicamente por no poder pagar fianzas de 2.500 dólares o menos». No obstante, el conjunto de medidas adoptadas, entre ellas la aplicación de PSA, redujeron la población en prisión preventiva a 9.000 personas en 2018, 6.000 menos que las registradas de media cada año en últimos 10 años⁸⁶.

⁸⁴ Marchena Gómez, M., *op. cit.*, pp. 53 y 54.

⁸⁵ Detalles de la herramienta de este párrafo y el anterior consultados en Advancing Pretrial Policy & Research, “Pretrial Research Summary: The Public Safety Assessment”, *Advancing Pretrial Policy & Research (APPR)*, 2021, pp. 1 y 2 (disponible en <https://www.advancingpretrial.org/resource/research/>; última consulta 24/03/2026).

⁸⁶ Anderson, C., Redcross, C., Valentine, E. y Miratrix, L., *Evaluation of Pretrial Justice System Reforms That Use the Public Safety Assessment: Effects of New Jersey’s Criminal Justice Reform*, MDRC Center for Criminal Justice Research, 2019, pp. 3 y 25 (disponible en <https://www.mdrc.org/work/publications/evaluation-pretrial-justice-system-reforms-use-public-safety->

A pesar de esto, el sistema no ha conseguido eliminar ciertas flaquezas. Un caso de uso que despertó la controversia hacia PSA fue la situación en un condado de Carolina del Norte (Mecklenburg County), donde se observó que a los ciudadanos negros se les mantenía en prisión provisional (*pretrial detention*) con mayor frecuencia que a los blancos aunque presentaran los mismos niveles de riesgo sin la evaluación de PSA⁸⁷.

Así, PSA vuelve a mostrar el sesgo racial de COMPAS, debido a que se alimenta de datos históricos generados por un sistema policial que puede contener discriminaciones raciales previas⁸⁸. La consecuencia de ello, y tal y como establece cierta doctrina, es que «si tales datos informan y nutren los sistemas actuales de predicción de riesgos, resulta muy difícil o incluso imposible evitar que los efectos perjudiciales de aquellos antiguos métodos ilegítimos o sesgados se repitan»⁸⁹.

Además, un estudio acerca del uso de PSA en Kentucky en 2018 reveló que el impacto del algoritmo en la reducción de la prisión preventiva inicial se reduce con el tiempo, ya que los jueces ejercen su discrecionalidad para ignorar los resultados de la herramienta. Esto permite hacer referencia en este punto a la presencia del sesgo del juez: el juicio de valor del magistrado sigue influyendo de forma desigual, volviendo a sus prejuicios o intuición de encarcelamiento, que en ocasiones mantiene las disparidades sociales y raciales⁹⁰.

1.1.3. LSI-R (Canadá)

Cerrando el bloque norteamericano, uno de los tres sistemas más influyentes en la justicia penal predictiva es el algoritmo LSI-R (*Level of Service Inventory-Revised*). Impulsado en Canadá por criminólogos, este algoritmo es una de las principales bases metodológicas que inspiraron el diseño del algoritmo *RisCanvi*, actualmente aplicado en las prisiones de Cataluña y que será objeto de análisis más adelante en este capítulo⁹¹.

[assessment-0](#); última consulta 24/03/2026).

⁸⁷ Advancing Pretrial Policy & Research, *op cit*, p. 5.

⁸⁸ Cuatrecasas Monforte, C., *op cit*, pp. 254 y 255; introduce el concepto de «*dirty police*» para hacer referencia a los procedimientos “dudosos” realizados a lo largo de la historia por la policía para recopilar información de los arrestados (información que nutre al sistema de IA): «en muchos casos empleaban datos incorrectos, obtenidos de manera ilegal o con prejuicios racistas o sociales».

⁸⁹ *Id.*

⁹⁰ Advancing Pretrial Policy & Research, *op cit*, p. 6.

⁹¹ Martínez Garay, L., “Tres sistemas de policía predictiva en España: VIOGÉN, RISCANVI y VERIPOL: Evaluación desde una perspectiva de derechos humanos”, *Publicacions De La Universitat De València*, 2026, p. 80 (<https://doi.org/10.7203/PUV-OA-9788411186605>).

LSI-R se fundamenta en el modelo RNR (Riesgo, Necesidad y Responsividad) y evalúa no solo la probabilidad de reincidencia, sino también las necesidades del individuo para orientar su tratamiento en la ejecución de la condena, que es su principal ámbito de aplicación. Para identificar las necesidades existenciales, el algoritmo analiza diez categorías del individuo, que incluyen tanto antecedentes penales como factores personales y sociales (situación financiera, empleo, relaciones personales, consumo de alcohol y drogas, etc.).

No obstante, aunque en la práctica judicial se centre en la concesión de permisos de salida y libertad condicional (ejecución de la sentencia)⁹², la sentencia del caso *Malenchik vs. State of Indiana* dio al algoritmo un papel relevante adicional en la determinación de la pena. Fue la primera vez que un tribunal se pronunció sobre la presencia de algoritmos predictivos en el proceso penal⁹³. La Corte Suprema de Indiana validó el uso de LSI-R como un elemento legítimo de apoyo para que los jueces dictasen la sentencia adecuada, definiendo la herramienta como una «fuente complementaria de información» para ayudar al tribunal a orientar «la forma en la que debe cumplirse la condena»⁹⁴.

En línea con las flaquezas observadas en los sistemas anteriores (sesgo de la IA), parte de la doctrina ha criticado en numerosas ocasiones la inclusión de factores sociales y personales en la predicción de riesgos que justifiquen las restricciones de derechos, tal y como ocurre en LSI-R. Muñoz Aranguren, magistrado del TS, contempla el riesgo de que la justicia penal predictiva haga avanzar a la sociedad hacia un «derecho penal de autor», lo que implicaría «castigar al condenado -al menos, en parte- en función de quién es, no estrictamente por lo que ha hecho»⁹⁵.

⁹² Sobre los detalles de la herramienta desarrollados en estas líneas y en el párrafo anterior, *vid.* Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., *op cit*, p. 280; y Martínez Garay, L., “Tres sistemas de policía predictiva...”, *op cit*, pp. 80 y 81.

⁹³ Martínez Garay, L., “Peligrosidad, algoritmos y due process...”, *op cit*, p. 494.

⁹⁴ Sentencia de la Corte Suprema de Indiana, *Malenchik v. State*, núm. 79S02-0908-CR-365, de 9 de junio de 2010 [versión electrónica – base de datos vLex. Ref: 928 N.E.2d 564 (Ind. 2010)] (disponible en <https://case-law.vlex.com/vid/malenchik-v-state-of-892370689>). Fecha de la última consulta: 24 de marzo de 2026.

⁹⁵ Muñoz Aranguren, A., *op cit*, p. 8.

1.2. Sistemas de predicción policial de riesgo delictivo

Tras el análisis de las herramientas que asisten directamente al órgano jurisdiccional en la evaluación del *periculum in mora*, es fundamental ampliar el foco de estudio a la fase pre-procesal o policial. Aunque los sistemas de policía predictiva operan en un estadio previo al proceso penal, su análisis es indispensable para este TFG, ya que los informes generados por estos algoritmos pueden incorporarse al atestado policial y condicionar la percepción inicial del juez sobre la peligrosidad del individuo y la necesidad de adoptar medidas cautelares⁹⁶. Además, analizar las flaquezas de estos sistemas englobados en el concepto de «justicia penal predictiva»⁹⁷ permite identificar problemas estructurales comunes que supongan una amenaza para el mantenimiento de las garantías de libertad y presunción de inocencia en sede judicial.

1.2.1. HART (Reino Unido)

Harm Assessment Risk Tool (HART) es una herramienta de IA empleada por la Policía de Durham en Reino Unido, que fue desarrollada por esta junto con la Universidad de Cambridge. A diferencia de los sistemas analizados anteriormente, HART se integra en la fase policial para ayudar a decidir si un sospechoso debe permanecer en prisión preventiva o si, en caso de presentar un riesgo moderado o bajo, puede ser derivado a un programa de rehabilitación (llamado *Checkpoint*). Para ello, evalúa el riesgo de reincidencia de un individuo (clasificado en bajo, moderado o alto riesgo) a través de 34 categorías de datos que incluyen factores como la edad, el sexo, los antecedentes penales, la profesión y el estado civil.

La herramienta se dio a conocer tras la denuncia de la organización Big Brother Watch en 2018, que calificó el análisis de riesgos de HART como «sesgado y discriminatorio», ya que examinaba entre sus datos el código postal de los individuos, lo que puede condicionar la clasificación de las personas en función del nivel socioeconómico y no solo por su conducta⁹⁸. El sesgo de la IA vuelve a cobrar protagonismo: la organización denunciante reveló que Durham Police «alimentaba el sistema (HART) con datos de

⁹⁶ Barona Vilar, S., “Algoritmización de la prueba y la decisión judicial en el proceso penal: ¿utopía o distopía?” en Arangüena Fanego, C., De Hoyos Sancho, M., Pillado González, E. (dirs.), Freitas, P. M. (coord.), *El proceso penal ante una nueva realidad tecnológica europea*, Aranzadi, Pamplona, 2023, pp. 149 y 150.

⁹⁷ *Vid.* concepto ampliado en la nota al pie nº 67.

⁹⁸ Sobre los detalles de la herramienta desarrollados en este párrafo y el anterior, *vid.* Barona Vilar, S., *op cit.*, p. 146 y Cuatrecasas Monforte, C., *op cit.*, pp. 249 y 250.

perfilado sociodemográfico de la agencia Experian»⁹⁹. Este elemento fue eliminado por la policía de Durham para asegurar la objetividad del sistema.

2. PRECEDENTES EN EL ORDENAMIENTO JURIDÍDICO ESPAÑOL

Tras examinar la situación del Derecho comparado acerca de algunos de los principales algoritmos de evaluación de riesgo, procede analizar ahora el ordenamiento jurídico español. El objeto de este análisis es valorar si existen ya en España antecedentes de estos sistemas que permitan anticipar el encaje constitucional y, sobre todo, los límites de una eventual utilización de sistemas de IA en la valoración del riesgo procesal para la adopción de medidas cautelares personales ya que, a día de hoy, aún no consta su utilización en este ámbito concreto.

2.1. VioGén

Entre los precedentes más relevantes en el contexto español destaca, en primer lugar, el sistema VioGén, un Sistema de Seguimiento Integral en los casos de Violencia de Género de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Nace en 2007 en cumplimiento de la LO 1/2004 de Medidas de Protección Integral contra la Violencia de Género como una herramienta de valoración de riesgo, y la doctrina lo define como «el algoritmo más desarrollado de cuantos utilizan nuestras fuerzas y cuerpos de seguridad», que en 2025 evolucionó a VioGén 2 incorporando mejoras de carácter técnico¹⁰⁰. Su función es calcular la probabilidad de que una mujer que ya ha denunciado vuelva a ser agredida por su pareja o expareja, permitiendo a la policía asignar niveles de protección proporcionales a dicha amenaza¹⁰¹.

VioGén opera a través de dos formularios cumplimentados por la policía: (i) el VPR (Valoración Policial del Riesgo): realizado tras la denuncia inicial y encargado de cuantificar «el grado de probabilidad de que la persona pueda seguir siendo objeto de

⁹⁹ Big Brother Watch Team, “A Closer Look at Experian Big Data and Artificial Intelligence in Durham Police”, *Big Brother Watch*, 6 de abril de 2018 (disponible en <https://bigbrotherwatch.org.uk/blog/a-closer-look-at-experian-big-data-and-artificial-intelligence-in-durham-police/>; última consulta 24/03/2026).

¹⁰⁰ Nota de prensa del Ministerio del Interior, “Interior diseña un nuevo modelo de respuesta policial a la violencia de género”, *La Moncloa: Web oficial del presidente del Gobierno y el Consejo de Ministros*, 15 de enero de 2025 (disponible en <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2025/150125-marlaska-redondo-sistema-viogen-2.aspx>; última consulta 24/03/2026).

¹⁰¹ Borges Blázquez, R., *op cit*, p. 393.

acoso»¹⁰², y (ii) el VPER (Valoración Policial de la Evolución del Riesgo): destinado a monitorizar el caso en el tiempo. El sistema emite un nivel de riesgo asociado al individuo tras analizar ciertos indicadores (antecedentes penales, características del agresor, vulnerabilidad de la víctima, etc.) y ese resultado se incorpora al atestado policial¹⁰³.

El atestado se remite al Juzgado de Violencia sobre la Mujer, donde el juez valorará la adopción de medidas cautelares, para lo que tendrá en cuenta el nivel de riesgo estimado por VioGén como instrumento auxiliar, sin ser determinante ni vinculante. Para la concesión de la orden de protección (art. 544 ter LECrim)¹⁰⁴, el juez valorará el resultado del algoritmo, pero lo hará junto con las declaraciones de la víctima y el investigado, los informes médicos de lesiones o los antecedentes penales, entre otros¹⁰⁵.

La doctrina destaca la capacidad de VioGén de «objetivar» el *periculum in mora*, lo que permite tomar decisiones más proporcionales y racionales¹⁰⁶. A pesar de esto, el fallo de la Sentencia de la Audiencia Nacional de 30 de septiembre de 2020 generó una gran crítica hacia este sistema, lo que permite analizar el riesgo que conlleva la aplicación de su resultado sin su previo estudio humano.

La Sala de lo Contencioso-Administrativo condenó al Ministerio del Interior tras el asesinato de una mujer cuyo riesgo había sido clasificado por la Guardia Civil como «no apreciado»¹⁰⁷. Para valorar el riesgo, la Audiencia Nacional expresa que los agentes rellenaban el formulario de VioGén y este daba una estimación del riesgo, aunque el sistema «permite la modificación al alza por los agentes si consideran que resulta

¹⁰² Pereira Puigvert, S., “La justicia y el proceso penal en clave algorítmica. Nuevos enfoques, nuevos riesgos”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, p. 72 (<https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03>).

¹⁰³ Montesinos García, A., “Inteligencia artificial en la justicia con perspectiva de género: amenazas y oportunidades”, *Actualidad Jurídica Iberoamericana*, n. 21, 2024, p. 589.

¹⁰⁴ *Cfr.* arts. 544 bis y 544 ter LECrim: **diferencia entre la medida cautelar del art. 544 bis y la orden de protección del 544 ter**: la orden de protección (art. 544 ter LECrim) se aplica a los casos de violencia doméstica dentro del ámbito familiar; mientras que las medidas cautelares del supuesto del art. 544 bis LECrim no sólo se adoptan en el ámbito familiar, sino frente a todos. Para acordar la orden de protección del art. 544 ter se debe escuchar a la víctima y al investigado y citar al Ministerio Fiscal, mientras que para las cautelares del 544 bis no es necesario. Además, la medida cautelar comprende únicamente medidas penales (como la prohibición de acercarse a la víctima), mientras que la orden de protección comprende además la posibilidad de dictar medidas civiles en ciertos supuestos (como el uso de la vivienda o la patria potestad).

¹⁰⁵ Borges Blázquez, R., *op cit*, p. 393.

¹⁰⁶ *Ibid.*, p. 402.

¹⁰⁷ *Vid.* Fundamento Jurídico Tercero de la Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 5ª) rec. 2187/2019, de 30 septiembre de 2020 [versión electrónica – base de datos Aranzadi. Ref: JUR/2020/290359; ECLI:ES:AN:2020:2350]. Fecha de la última consulta: 24 de marzo de 2026.

necesario asignar un nivel de riesgo más alto para una mejor protección de la víctima»¹⁰⁸.

La sentencia relata que el sistema falló al no valorar adecuadamente indicios objetivos (antecedentes de maltrato en el país de origen o testimonios de trabajadoras sociales) y que la actuación de la policía al aceptar el resultado de VioGén derivó en un incumplimiento de la obligación estatal de protección al no adoptar la orden de protección solicitada por la víctima¹⁰⁹.

Sin embargo, entre otras de las flaquezas identificadas del sistema, Martínez Garay destaca que VioGén está intencionadamente sesgado hacia los «falsos positivos». El sistema fue diseñado para maximizar la sensibilidad y no dejar a mujeres desprotegidas, lo que implica que gran parte de los sujetos que son calificados como de alto riesgo nunca vuelven a agredir. Y aunque esto se pueda asumir en la fase policial de protección, si el juez lo usara de manera automática para aplicar las restricciones (sin una revisión previa) podría ser muy perjudicial para la libertad del individuo y sus derechos fundamentales¹¹⁰.

Además, Borges Blázquez hace referencia de nuevo (identificada ya en el sistema COMPAS) a la opacidad del VioGén (*black box*) y reclama la falta de transparencia por conocerse los factores analizados para la evaluación del riesgo, pero no el peso exacto que el algoritmo otorga a cada uno, lo que puede dificultar su derecho de defensa «al no poder argumentar contra la máquina a qué se debe el riesgo de reincidencia»¹¹¹.

2.2. RisCanvi

El sistema RisCanvi (acrónimo de riesgo (*risc*) y cambio (*canvi*) en catalán) fue implementado en las prisiones de Cataluña en el año 2009 con el objetivo de predecir el riesgo de reincidencia violenta de la población reclusa, incluso para aquellos individuos que se encuentren cumpliendo la condicional. Su ámbito de aplicación, por tanto, es penitenciario para los individuos privados de su libertad o en situación de prisión preventiva (sin condena firme)¹¹².

¹⁰⁸ *Id.*

¹⁰⁹ Montesinos García, A., *op cit*, p. 590.

¹¹⁰ Martínez Garay, L., “Tres sistemas de policía predictiva...”, *op cit*, p. 21.

¹¹¹ Borges Blázquez, R., *op cit*, p. 399.

¹¹² Desarrollado en el informe del Centro de Estudios Políticos y Constitucionales (CEPC), “Inteligencia artificial y justicia”, *Web del Centro de Estudios Políticos y Constitucionales dependiente del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes*, 2025, p. 18 (disponible en <https://www.cepc.gob.es/documentacion/informes-tematicos>; última consulta 24/03/2026), cuyo contenido se basa en: Generalitat de Catalunya, Departament de Justícia i Qualitat Democràtica, “Protocol de valoració del risc (RisCanvi)”, s. f. (disponible en

Basado en el modelo RNR (Riesgo, Necesidad y Responsividad) desarrollado en el sistema norteamericano LSI-R, su función principal se da en la fase de ejecución de la pena (una vez existe condena firme): su predicción de riesgo sirve de guía para el juez a la hora de tomar decisiones como la progresión al tercer grado, la concesión de permisos de salida y el acceso a la libertad condicional¹¹³.

Una investigación del diario El Confidencial en 2024 reveló por primera vez el peso exacto de las variables que RisCanvi analizaba para valorar el riesgo de reincidencia. El estudio expuso opiniones de expertos como Castillo que expresaron que la herramienta «no pasaría hoy los filtros exigidos por Europa» de transparencia y calidad de los datos debido al uso de «datos de entrenamiento desactualizados y la baja calidad de sus predicciones sobre los grupos menos representados en las prisiones de Cataluña, como las mujeres y los extranjeros»¹¹⁴.

Además, el artículo aporta el testimonio de Jesús, un preso en libertad condicional que confesó que llevaba ya dos años en prisión la primera vez que escuchó la palabra RisCanvi cuando le entregaron un informe sobre «los permisos a los que podría optar durante su condena». Confesó que desde ese momento y durante su tiempo restante en prisión, su objetivo fue constante: «*tenía que bajar el RisCanvi*». Así, este estudio demostró la falta de transparencia de RisCanvi, y que los presos ni siquiera estaban siendo informados de la existencia del algoritmo ni de cómo podía afectar a sus derechos.

2.3. VeriPol

Por último, y para concluir el análisis de la justicia predictiva en el proceso penal español, es preciso analizar VeriPol (acrónimo de “Verificación Policial”), que constituye la primera herramienta a nivel mundial que emplea IA para detectar denuncias falsas por robo con violencia e intimidación y hurtos por el método del «tirón»¹¹⁵.

https://justicia.gencat.cat/ca/ambits/reinsercio_i_serveis_penitenciaris/serveis_penitenciaris/RisCanvi/; última consulta 24/03/2026).

¹¹³ Gimeno Beviá, J., *op cit*, p. 152.

¹¹⁴ Arandía, P. J., Ley, M., Luengo, J., Martín, L., Mateo, M., Ortega, M. G., Sisqués, S., “Un algoritmo define el futuro de los presos en Cataluña: ahora sabemos cómo funciona”, *El Confidencial*, 24 de abril de 2024 (disponible en https://www.elconfidencial.com/tecnologia/2024-04-24/riscanvi-algoritmo-cataluna-prisiones-presos-inteligencia-artificial_3871170/; última consulta: 24/03/2026).

¹¹⁵ Nota de prensa de la Policía Nacional, “La Policía Nacional pone en funcionamiento la aplicación informática VeriPol para detectar denuncias falsas”, *Portal web de la Policía Nacional*, 27 de octubre de 2018 (disponible en https://www.policia.es/es/comunicacion_prensa_detalle.php?ID=4433&idiomaActual=es#; última consulta 24/03/2026).

Fue desarrollada por la Policía Nacional en 2018 y desmantelada en octubre de 2024 por carecer de validez en los procedimientos judiciales. Aunque fue empleada en el ámbito policial, es preciso analizarla en este TFG ya que el abandono del sistema se debió a la deficiencia en el cumplimiento de requisitos europeos de transparencia y supervisión exigidos por el Reglamento de IA para este tipo de sistemas «de alto riesgo»¹¹⁶.

El sistema no analizaba directamente la declaración del ciudadano, sino el texto del atestado redactado por el agente de policía, y tras su análisis, estimaba la probabilidad de que la denuncia fuera falsa. Con este *modus operandi*, VeriPol fue objeto de crítica por la doctrina. Martínez Garay denuncia el riesgo del sistema de sufrir un sesgo de confirmación, ya que procesaba el texto escrito por el policía y no las palabras literales del denunciante. Esto implica que la percepción o impresión que tuviera el agente sobre la credibilidad del relato podía influir en su forma de redactar el atestado, y con ello, la probabilidad que estimara el sistema simplemente confirmaba la sospecha inicial del agente¹¹⁷.

La retirada de VeriPol parece procedente ya que, además, fue calificado como el sistema más opaco de los tres algoritmos españoles analizados: «es la herramienta de la que menos información se dispone», lo que podía generar indefensión al denunciante¹¹⁸.

La observancia de los precedentes existentes tanto en el Derecho comparado como en el ámbito nacional sienta las bases sobre las que modelar la posible implementación de un sistema de IA en el proceso penal que auxilie al juez a predecir medidas cautelares, cuya admisibilidad en el ordenamiento jurídico español será analizada a continuación.

¹¹⁶ Véase la noticia del diario *El País* de 19 de marzo de 2025 (nota al pie nº 15).

¹¹⁷ Martínez Garay, L., “Tres sistemas de policía predictiva...”, *op cit*, pp. 138 y 146.

¹¹⁸ *Ibid.*, p. 24.

CAPÍTULO IV. LA IA ANTE EL MODELO ESPAÑOL DE JUSTICIA CAUTELAR

Una vez examinado el régimen jurídico de las medidas cautelares personales, el marco normativo europeo y español sobre IA y las deficiencias de los sistemas de evaluación algorítmica de riesgo, corresponde analizar su encaje en el proceso penal español. Este capítulo no pretende reiterar los problemas ya identificados, sino valorar su alcance desde la perspectiva de los derechos fundamentales y de la estructura garantista de la justicia cautelar, para determinar si la LECrim ofrece hoy una base suficiente para su incorporación o si, por el contrario, es necesaria una reforma.

1. TENSIONES ENTRE LAS GARANTÍAS PROCESALES Y LA *BLACK BOX* DE LOS SISTEMAS DE IA

1.1. Transición a un derecho penal de autor

Las tensiones entre las garantías del proceso y la *black box* propia de los sistemas de IA surgen debido a la flaqueza de los datos grupales que tienden a utilizar estos sistemas. Ya ha sido analizado por la doctrina que ciertos sistemas como COMPAS o RisCanvi, en la práctica, no evalúan al individuo por sí mismo, sino que tienden a asignar una puntuación de riesgo basada en el comportamiento histórico de grupos de referencia similares¹¹⁹. Esto implica que el sujeto sea juzgado por quién es o a qué colectivo pertenece, y no por sus actos concretos (transición a un «derecho penal de autor»¹²⁰).

Y es que, además, esa generalización puede derivar en que las restricciones de libertad se fundamenten en «comportamientos predichos» y no en hechos reales, lo que pondría en riesgo el derecho a la presunción de inocencia del individuo (considerando 42 RIA).

Se ha podido apreciar en el análisis realizado de los algoritmos que, hasta hoy, estos sistemas han operado en base a la estandarización de perfiles, y es que la LECrim en su art. 503¹²¹ exige para la adopción de la prisión provisional, que cada decisión sobre la libertad atienda a las circunstancias únicas del investigado¹²².

¹¹⁹ Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., *op cit*, p. 289.

¹²⁰ *Vid.* nota al pie nº 95.

¹²¹ Art. 503.1.2º LECrim: “1. La prisión provisional sólo podrá ser decretada cuando concurren los siguientes requisitos: (...) 2.º Que aparezcan en la causa motivos bastantes para creer responsable criminalmente del delito **a la persona contra quien se haya de dictar** el auto de prisión (...)”.

¹²² Rangugni, M. C., “Inteligencia Artificial en las sentencias de la justicia criminal” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración*

1.2. Riesgo de indefensión

Esa estandarización se ve agravada por el fenómeno de la «caja negra» o falta de transparencia algorítmica (*black box*). Como evidenció el caso *Loomis*, el secreto comercial del sistema COMPAS, «al ser un instrumento patentado», impide que los individuos conozcan el peso real de las variables empleadas para predecir el riesgo¹²³.

En España, sistemas como RisCanvi o VioGén presentan una opacidad similar y la doctrina ha denunciado en numerosas ocasiones la indefensión que esto genera en el individuo¹²⁴.

Sin embargo, ese riesgo de indefensión encuentra un límite en la doctrina del Tribunal Europeo de Derechos Humanos (TEDH) en la sentencia *Buzadji v. Republic of Moldova*. Tal y como sentenció el TEDH «los motivos referidos por los Tribunales nacionales para ordenar la detención o la prolongación de la detención no pueden estar estereotipados ni ser abstractos»¹²⁵. Esto implica que la adopción de las decisiones cautelares debe estar expresamente motivada.

Además, el TEDH reitera la importancia del juicio de proporcionalidad que debe realizar el magistrado para privar de libertad a un individuo, debiendo aportar motivos «pertinentes y suficientes» ante la imposición de la medida cautelar¹²⁶.

Así, si el juez se limita a validar el resultado de un sistema de IA que él mismo no puede explicar con detalle (*black box*), estaría incurriendo en la falta de motivación convincente que exige el TEDH a los tribunales nacionales y violando el principio de proporcionalidad al no poder justificar la necesidad de la medida cautelar¹²⁷.

Por otro lado, la opacidad del sistema de IA podría romper con el estándar de previsibilidad y seguridad jurídica asentado por el TEDH en el asunto *Scoppola v. Italia* (n.º 2). En este caso, el Tribunal estableció que cualquier sujeto debe poder saber, a partir del tenor de la norma, qué actos le hacen responsable y qué consecuencias penales se le

de justicia: la policía predictiva y la justicia predictiva, Jusbairens, Buenos Aires, 2025, p. 122.

¹²³ Traducido por Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., *op cit*, p. 288 de la Sentencia de la Corte Suprema de Wisconsin, *State v. Loomis*, núm. 2015AP157-CR...

¹²⁴ Borges Blázquez, R., *op cit*, pp. 403 y 404.

¹²⁵ *Vid.* Fundamento de hecho nº 59 (“La ley y la práctica de los Estados Miembros del Consejo De Europa”) de la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), demanda núm. 23755/07, *Buzadji v. Republic of Moldova*, de 5 de julio de 2016 [versión electrónica – base de datos HUDOC. Ref: 001-164928]. Fecha de la última consulta: 24 de marzo de 2026.

¹²⁶ *Ibid.*, fundamento jurídico nº 102.

¹²⁷ *Ibid.*, fundamento jurídico nº 122.

aplicarán. El TEDH define esto como *foreseeability of the criminal law* (o «previsibilidad del derecho penal»), es decir, que las consecuencias de las decisiones procesales sean previsibles para el investigado¹²⁸.

En el ámbito de la justicia penal predictiva, si el riesgo de un individuo es evaluado por un sistema de IA cuyo funcionamiento es desconocido (como sucedió con la opacidad de COMPAS), no podrá evaluar de forma real y efectiva las consecuencias de su situación de libertad, ni prever ese resultado al no contar con toda la información del algoritmo¹²⁹.

La libertad del individuo dependería, por tanto, de la arbitrariedad del sistema de IA como consecuencia de la «sumisa aceptación» por parte de la justicia «a su pronóstico de peligrosidad»¹³⁰.

2. SESGO DE AUTOMATIZACIÓN Y EXCLUSIVIDAD JURISDICCIONAL

El principio de exclusividad jurisdiccional, consagrado en el art. 117.3 CE y en la LOPJ¹³¹, establece que la potestad de juzgar y hacer ejecutar lo juzgado «corresponde exclusivamente a Juzgados y Tribunales»¹³². Dijo el ya referenciado magistrado del Tribunal Supremo Manuel Marchena, que la labor del juzgador se trata de una tarea genuinamente humana que requiere sensibilidad ante el valor de la justicia¹³³.

Ante este panorama, la irrupción de la IA introduce el riesgo del sesgo de automatización¹³⁴, concepto analizado con el nuevo marco legislativo europeo (capítulo II), y que puede provocar que el juez delegue materialmente su razonamiento en el algoritmo y omita el análisis exhaustivo de las circunstancias del caso.

En esta línea, se ha observado en la práctica de VioGén que en el 95% de los casos «el personal de las Fuerzas y Cuerpos de Seguridad está de acuerdo con el riesgo asignado»¹³⁵, es decir, que existe el riesgo de que acepten la valoración del sistema

¹²⁸ Vid. Fundamento jurídico nº 99 y 102 de la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), demanda núm. 10249/03, Scoppola v. Italy (nº 2), de 17 de septiembre de 2009 [versión electrónica – base de datos HUDOC. Ref: 001-94135]. Fecha de la última consulta: 24 de marzo de 2026.

¹²⁹ *Ibid.*, fundamento jurídico nº 139.

¹³⁰ Marchena Gómez, M., *op. cit.*, p. 57.

¹³¹ Vid. Art. 1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985), que reafirma la división de poderes del Estado.

¹³² Castillo Felipe, R., Tomás Tomás, S., “Proceso penal e inteligencia artificial: prevenciones en torno a su futura aplicación en la fase de juicio oral” en Peris Riera, J. M., Massaro, A. (coords), *Derecho Penal, Inteligencia Artificial y Neurociencias/ Diritto Penale, Intelligenza Artificiale e Neuroscienze*, Roma Tre-Press, Roma, 2023, p. 218.

¹³³ Marchena Gómez, M., *op. cit.*, p. 70.

¹³⁴ Vid. nota al pie nº 47.

¹³⁵ González Álvarez, J. L., López-Ossorio, J. J., Urruela, C., Rodríguez-Díaz, M., “Integral Monitoring

automáticamente sin un análisis detenido. El problema reside en que, si esta inercia debida a la confianza en el sistema se traslada al ámbito judicial, el algoritmo pasaría a sustituir al juez en lugar de ser un apoyo para el mismo.

Parte de la doctrina ya ha denunciado situaciones similares en las que se ha producido una «sumisión judicial al algoritmo transformado en ley». Esto ha sucedido con las pruebas periciales: «si actualmente el juez se halla en muchas ocasiones abrumado por las pruebas periciales, sin verdaderas herramientas o criterios para evaluar críticamente la opinión de los expertos, igual fenómeno se reproducirá al acudir a la IA»¹³⁶. Es decir, que el juez podría llegar a verse tentado por la respuesta del algoritmo y guiarse por ella¹³⁷.

Y es que esa falta de criterio del juez para evaluar la veracidad y calidad de la respuesta del sistema de IA se debe a la falta de «alfabetización» de la administración de justicia en inteligencia artificial (*AI literacy*). Como define la investigación científica, el concepto «*AI literacy*» se refiere a la capacidad del individuo de evaluar críticamente el contenido generado por sistemas de IA para evitar un exceso de confianza en sus resultados¹³⁸.

Por ello, con la inminente entrada de estos sistemas en el proceso penal, es imprescindible educar y entrenar a los jueces que apliquen las respuestas de la IA para que aprendan a reconocer sus sesgos, límites y posibles errores, y puedan someter sus resultados a una valoración crítica propia.

3. LA INSUFICIENCIA DE LA LECRIM: UN HORIZONTE DE REFORMA

Son varias las reformas que ha experimentado el proceso penal español para adaptarse a la era digital. Desde la reforma de la LOPJ a través de la LO 16/1994¹³⁹, que introdujo la posibilidad de usar medios electrónicos en los juzgados; la posterior reforma de la LECrim mediante la LO 13/2003¹⁴⁰, con la regulación de la videoconferencia en las actuaciones judiciales; hasta la gran revolución de la conocida como «ley del papel

System in Cases of Gender Violence VioGén System”, *Behavior & Law Journal*, vol. 4, n. 1, 2018, p. 37 (<https://doi.org/10.47442/blj.v4.i1.56>), citado en Borges Blázquez, R., *op cit*, p. 395.

¹³⁶ Castillo Felipe, R., Tomás Tomás, S., *op cit*, p. 228.

¹³⁷ Así impactó sobre los agentes de policía el resultado de VioGén en el escándalo expuesto anteriormente (*vid.* nota al pie nº 107) sentenciado por la Audiencia Nacional en 2020.

¹³⁸ Oliveira, L., Tavares, C., Strzelecki, A., Silva, M., “Prompting Minds: Evaluating How Students Perceive Generative AI's Critical Thinking Dispositions”, *Electronic Journal of E-learning*, vol. 23, núm. 1, 2025, p. 11 (<https://doi.org/10.34190/ejel.23.2.3986>).

¹³⁹ Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 9 de noviembre de 1994).

¹⁴⁰ Ley Orgánica 13/2003, de 24 de octubre, de reforma de la Ley de Enjuiciamiento Criminal en materia de prisión provisional (BOE 27 de octubre de 2003).

ceros»¹⁴¹ (Ley 42/2015) que impulsó el Expediente Judicial Electrónico¹⁴². Sin embargo, estas reformas se centraron en la gestión documental eficaz y en la forma de comunicación entre la administración de justicia y las partes.

Por otro lado, la LO 13/2015¹⁴³ reformó la LECrim para situarla “al día” en la regulación de medidas de investigación tecnológica sobre: interceptación de comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales, la utilización de dispositivos de seguimiento y localización, etc. Sin embargo, esta reforma ha quedado anticuada a día de hoy, ya que la LO 7/2021 introdujo la prohibición de las decisiones automatizadas (a las que se hizo referencia en el capítulo II)¹⁴⁴.

Otro texto de relevancia es el Real Decreto-ley 6/2023 (capítulo II), que, aunque sea una regulación importante acerca de las actuaciones asistidas por algoritmos, la doctrina ha dudado de su fiabilidad al afectar directamente a derechos fundamentales y no tener rango de Ley Orgánica¹⁴⁵.

Sin embargo, la esperanza de reforma de la LECrim ante el uso en sede judicial de sistemas de IA de evaluación de riesgo nació en 2020 con el Anteproyecto de Ley de Enjuiciamiento Criminal¹⁴⁶. Aprobado el 24 de noviembre por el Consejo de Ministros, el texto contempló por primera vez la regulación de los «instrumentos de valoración del riesgo de reincidencia» en su art. 485¹⁴⁷.

Aunque su tramitación a proyecto de ley no llegó a producirse, el reciente Proyecto de Ley Orgánica de Enjuiciamiento Criminal de 14 de noviembre de 2025¹⁴⁸ ha vuelto a consolidar la regulación de este tipo de instrumentos de la misma manera que lo hizo el

¹⁴¹ Bueno de Mata, F., “Interoperabilidad de sistemas de gestión procesal y debido proceso: experiencias a nivel nacional y europeo para alcanzar una verdadera digitalización de la justicia” en Llorente Sánchez-Arjona, M., Calaza López, S. (dirs.), Muñelo Cobo, J. C. (coord.), Digitalización de la justicia: Prevención, Investigación y Enjuiciamiento, Thomson Reuters-Aranzadi, Pamplona, 2022, p. 158.

¹⁴² Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 6 de octubre de 2015).

¹⁴³ Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE 6 de octubre de 2015).

¹⁴⁴ Art. 14 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE 27 de mayo de 2021): “1. Están prohibidas las decisiones **basadas únicamente en un tratamiento automatizado...**”.

¹⁴⁵ Bueno de Mata, F., *op cit.*, p. 21.

¹⁴⁶ Anteproyecto de Ley de Enjuiciamiento Criminal, de 26 de enero de 2021 (versión para información pública disponible en la web del Ministerio de Justicia).

¹⁴⁷ Muñoz Aranguren, A., *op cit.*, p. 4.

¹⁴⁸ Proyecto de Ley Orgánica de Enjuiciamiento Criminal, de 14 de noviembre de 2025, XV Legislatura, Serie A, núm. 74-I (BOCG 14 de noviembre de 2025).

Anteproyecto¹⁴⁹:

«Artículo 491. Instrumentos de valoración del riesgo de violencia o reincidencia.

1. Los instrumentos de valoración del riesgo de violencia o reincidencia deberán incluir todos los parámetros estadísticos que permitan **evaluar tanto su fiabilidad como su capacidad predictiva** y se utilizarán protocolos de evaluación del riesgo que contengan una **metodología científicamente sustentada**.

2. Dichos instrumentos **especificarán** el tamaño de la población con la que se han construido, las variables utilizadas como factores de riesgo, los criterios de medición empleados para ponderar dichos factores asignando puntuaciones, y el tiempo de validez de la predicción. También habrán de identificar los estudios de validación realizados».

Este precepto exige que tales herramientas incluyan todos los parámetros estadísticos necesarios para poder evaluar su fiabilidad y capacidad predictiva y que cuenten con una metodología científica sustentada. Lo que busca este artículo es abandonar la *black box* de los sistemas de IA para alcanzar la máxima transparencia. Ahora bien, tanto el Anteproyecto como el actual Proyecto sitúan esta regulación en la sección de «reglas especiales sobre prueba pericial», no dentro del régimen cautelar.

Por todo ello, aunque se ha valorado la integración de herramientas predictivas en la fase pericial del proceso, la LECrim aún no se ha pronunciado sobre el procesamiento de datos en los sistemas de IA, y menos aún sobre aquellos que pudieran auxiliar al juez en la adopción de medidas cautelares.

El análisis de la situación procesal española permite confirmar la tesis de Manuel Marchena Gómez sobre la «insuficiencia» del derecho codificado histórico¹⁵⁰, en particular, el de la Ley de Enjuiciamiento Criminal española para enfrentarse a las nuevas tecnologías, y en este caso, a la incorporación de sistemas de IA de evaluación de riesgo como apoyo al juez en decisiones cautelares.

¹⁴⁹ La única diferencia entre ambos arts. 485 y 491 del Anteproyecto de Ley 2020 y del Proyecto de Ley de 2025, respectivamente, es que al apartado 1 se le añadió esta última frase en 2025: «y se utilizarán protocolos de evaluación del riesgo que contengan una metodología científicamente sustentada».

¹⁵⁰ Marchena Gómez, M., *op. cit.*, p. 7.

CONCLUSIONES

Si algo revela este TFG es que hace mucho tiempo que el verdadero problema no consiste en decidir si la IA entrará o no en la justicia penal. La cuestión decisiva es en qué condiciones puede el ordenamiento jurídico español permitir su entrada cuando lo que está en juego no es simplemente una mejora organizativa, sino la libertad de una persona que todavía no ha sido condenada. Será en este momento entonces, en el ámbito de las medidas cautelares personales, donde el desarrollo tecnológico debe dejar paso a la máxima exigencia jurídica.

La promesa de la IA resulta muy llamativa. Frente a un juicio humano atravesado por intuiciones, inercias, cansancio, prejuicios y automatismos, un sistema de apoyo al juez podría aportar orden, consistencia y una objetivación del *periculum in mora*. Negarlo sería ingenuo.

Pero igual de ingenuo sería ignorar la otra cara de la moneda: los sistemas analizados a lo largo de este Trabajo muestran que la IA no nace neutral como prevé la nueva regulación europea de estos sistemas. En lugar de ello, aprende de realidades sesgadas, simplifica a los individuos mediante patrones grupales, y su opacidad es difícilmente compatible con un proceso penal garantista. PSA, HART o VioGén son una advertencia de ello.

Por ello, estoy a favor de introducir la IA en este ámbito únicamente como herramienta auxiliar de apoyo a la decisión del juez, nunca como una autoridad paralela ni, mucho menos, como una decisión automática. En las decisiones cautelares, aquellas en las que el Estado se plantea restringir la libertad antes de que exista una sentencia firme, la decisión debe seguir siendo radicalmente humana y motivada.

Desde esta perspectiva, mi propuesta para un eventual sistema futuro de IA de evaluación de riesgo es que sea diseñado como *colorblind*: sin valoración de raza ni de nacionalidad. El objetivo es impedir que el cálculo del riesgo reproduzca discriminaciones como las que han aflorado en precedentes como COMPAS o RisCanvi.

Aunque, de poco serviría eliminar esas variables si el sistema sigue alcanzando el mismo resultado a través de otras variables, como el entorno socioeconómico, el código postal o patrones históricos policiales y penitenciarios ya contaminados.

En consecuencia, el proceso penal español solo podría asumir esta innovación tras una reforma legislativa clara y garantista. La LECrim, tal y como hoy se encuentra, no ofrece una base suficiente para un uso tan delicado. Hacen falta reglas expresas sobre

transparencia, acceso de las partes al funcionamiento del sistema, control judicial real y preservación plena de los derechos de defensa, contradicción y presunción de inocencia.

En definitiva, la modernización del proceso penal no debe consistir en sustituir el juicio jurídico por la probabilidad de un algoritmo, sino en someter la tecnología al Derecho. La IA puede entrar en la justicia cautelar, pero solo si las garantías del individuo persisten. Innovar sobre la decisión que nos hace libres no puede significar arriesgar nuestros derechos, sino protegerlos mejor.

BIBLIOGRAFÍA

1. LEGISLACIÓN

1.1. ESPAÑA

Constitución Española. Boletín Oficial del Estado nº 311, de 29 de diciembre de 1978.

Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 6 de octubre de 2015).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).

Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 9 de noviembre de 1994).

Ley Orgánica 13/2003, de 24 de octubre, de reforma de la Ley de Enjuiciamiento Criminal en materia de prisión provisional (BOE 27 de octubre de 2003).

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE 6 de octubre de 2015).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE 27 de mayo de 2021).

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (Gaceta de Madrid nº 260, de 17 de septiembre de 1882).

Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (BOE 9 de noviembre de 2023).

Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (BOE 20 de diciembre de 2023).

1.1.1. PROYECTOS Y ANTEPROYECTOS DE LEY

Anteproyecto de Ley de Enjuiciamiento Criminal, de 26 de enero de 2021 (versión para información pública disponible en la web del Ministerio de Justicia).

Proyecto de Ley Orgánica de Enjuiciamiento Criminal, de 14 de noviembre de 2025, XV Legislatura, Serie A, núm. 74-1 (BOCG 14 de noviembre de 2025).

1.2. UNIÓN EUROPEA

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE 4 de mayo de 2016).

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 y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 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) (DO L, 2024/1689, de 12 de julio de 2024) (DOUE 12 de julio de 2024).

2. JURISPRUDENCIA

2.1. ESPAÑA

2.1.1. AUDIENCIA NACIONAL

Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 5ª) rec. 2187/2019, de 30 septiembre de 2020 [versión electrónica – base de datos Aranzadi. Ref: JUR\2020\290359; ECLI:ES:AN:2020:2350]. Fecha de la última consulta: 24 de marzo de 2026.

2.1.2. TRIBUNAL CONSTITUCIONAL

Sentencia del Tribunal Constitucional (Sala Primera) núm. 207/1996, de 16 de diciembre de 1996 [versión electrónica – BOE. Ref: BOE-T-1997-1175]. Fecha de la última consulta: 24 de marzo de 2026.

Sentencia del Tribunal Constitucional (Pleno) núm. 184/2003, de 23 de octubre de 2003

[versión electrónica – BOE. Ref: BOE-T-2003-20770]. Fecha de la última consulta: 24 de marzo de 2026.

2.1.3. TRIBUNAL SUPREMO

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 159/1996, de 24 de febrero de 1996 [versión electrónica – base de datos Cendoj. Roj: STS 1172/1996; ECLI:ES:TS:1996:1172]. Fecha de la última consulta: 24 de marzo de 2026.

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 845/1998, de 18 de junio de 1998 [versión electrónica – base de datos Cendoj. Roj: STS 4049/1998; ECLI:ES:TS:1998:4049]. Fecha de la última consulta: 24 de marzo de 2026.

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 578/2012, de 26 de junio de 2012 [versión electrónica – base de datos Cendoj. Roj: STS 5698/2012; ECLI:ES:TS:2012:5698]. Fecha de la última consulta: 24 de marzo de 2026.

Auto del Tribunal Supremo (Sala de lo Penal, Sección 1ª), rec. 20907/2017, de 18 de junio de 2018 [versión electrónica – base de datos Cendoj. Roj: ATS 6831/2018; ECLI:ES:TS:2018:6831A]. Fecha de la última consulta: 24 de marzo de 2026.

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 580/2021, de 1 de julio de 2021 [versión electrónica – base de datos Cendoj. Roj: STS 2834/2021; ECLI:ES:TS:2021:2834]. Fecha de la última consulta: 24 de marzo de 2026.

Auto del Tribunal Supremo (Sala de lo Penal, Sección 1ª) núm. 1252/2021, de 25 de noviembre de 2021 [versión electrónica – base de datos Cendoj. Roj: ATS 16740/2021; ECLI:ES:TS:2021:16740A]. Fecha de la última consulta: 24 de marzo de 2026.

2.2. UNIÓN EUROPEA

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), demanda núm. 10249/03, *Scoppola v. Italy (nº 2)*, de 17 de septiembre de 2009 [versión electrónica – base de datos HUDOC. Ref: 001-94135]. Fecha de la última consulta: 24 de marzo de 2026.

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), demanda núm. 23755/07, *Buzadji v. Republic of Moldova*, de 5 de julio de 2016 [versión electrónica – base de datos HUDOC. Ref: 001-164928]. Fecha de la última

consulta: 24 de marzo de 2026.

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera), asunto C-634/21, *SCHUFA Holding (Scoring)*, de 7 de diciembre de 2023 [versión electrónica – EUR-Lex. ECLI:EU:C:2023:957]. Fecha de la última consulta: 24 de marzo de 2026.

2.3. JURISPRUDENCIA EXTRACOMUNITARIA

Sentencia de la Corte Suprema de Indiana, *Malenchik v. State*, núm. 79S02-0908-CR-365, de 9 de junio de 2010 [versión electrónica – base de datos vLex. Ref: 928 N.E.2d 564 (Ind. 2010)] (disponible en <https://case-law.vlex.com/vid/malenchik-v-state-of-892370689>). Fecha de la última consulta: 24 de marzo de 2026.

Sentencia de la Corte Suprema de Wisconsin, *State v. Loomis*, núm. 2015AP157-CR, de 13 de julio de 2016, [versión electrónica – base de datos vLex. Ref: 371 Wis.2d 235, 881 N.W.2d 749 (Wis. 2016)] (disponible en <https://case-law.vlex.com/vid/state-v-loomis-no-888404547>). Fecha de la última consulta: 24 de marzo de 2026.

3. OBRAS DOCTRINALES

Álvarez Buján, M. V., “Inteligencia artificial y medidas cautelares en el proceso penal: tutela judicial efectiva y autodeterminación informativa en potencial riesgo”, *Revista Española de Derecho Constitucional*, vol. 127, 2023, pp. 177-207 (<https://doi.org/10.18042/cepc/redc.127.06>).

Barona Vilar, S., “Algoritmización de la prueba y la decisión judicial en el proceso penal: ¿utopía o distopía?” en Arangüena Fanego, C., De Hoyos Sancho, M., Pillado González, E. (dirs.), Freitas, P. M. (coord.), *El proceso penal ante una nueva realidad tecnológica europea*, Aranzadi, Pamplona, 2023, pp. 133-161.

Borges Blázquez, R., “Algoritmización de la concesión de medidas cautelares en el proceso penal para la protección de víctimas de violencia de género. ¿Es capaz VIOGEN de interpretar el ‘periculum in mora’?”, *Actualidad Jurídica Iberoamericana*, n. 21, 2024, pp. 384-407.

Bueno de Mata, F., “Interoperabilidad de sistemas de gestión procesal y debido proceso: experiencias a nivel nacional y europeo para alcanzar una verdadera digitalización

de la justicia” en Llorente Sánchez-Arjona, M., Calaza López, S. (dirs.), Muínelo Cobo, J. C. (coord.), *Digitalización de la justicia: Prevención, Investigación y Enjuiciamiento*, Thomson Reuters-Aranzadi, Pamplona, 2022, pp. 151-178.

Bueno de Mata, F., “Sistemas de gestión procesal, inteligencia artificial generativa y justicia orientada al dato: retos y desafíos”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, pp. 11-32 (<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.01>).

Calaza López, S., “Transición digital de la justicia” en Llorente Sánchez-Arjona, M., Calaza López, S. (dirs.), Muínelo Cobo, J. C. (coord.), *Digitalización de la justicia: Prevención, Investigación y Enjuiciamiento*, Thomson Reuters-Aranzadi, Pamplona, 2022, pp. 27-56.

Castillo Felipe, R., Tomás Tomás, S., “Proceso penal e inteligencia artificial: prevenciones en torno a su futura aplicación en la fase de juicio oral” en Peris Riera, J. M., Massaro, A. (coords), *Derecho Penal, Inteligencia Artificial y Neurociencias/ Diritto Penale, Intelligenza Artificiale e Neuroscienze*, Roma Tre-Press, Roma, 2023, pp. 215-245.

De Luca, J. A., “Prólogo e introducción” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, pp. 9-11.

Dorado Ferrer, J., “Simón Castellano, Pere, Justicia cautelar e inteligencia artificial: La Alternativa a los atávicos heurísticos Judiciales, J. M. Bosch Editor, Barcelona, 2021, 260 pp., ISBN 978-84-123154-0-0”, *Estudios De Deusto*, vol. 69, n. 2, 2021, pp. 347-352 ([https://doi.org/10.18543/ed-69\(2\)-2021pp347-352](https://doi.org/10.18543/ed-69(2)-2021pp347-352)).

Ensel, L., “Las sentencias algorítmicas frente al principio de culpabilidad y el derecho a ser oído en el proceso” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, pp. 233-248.

García Sánchez, M. D., “La necesidad de regulación de una nueva tipología cautelar frente a la delincuencia en el entorno digital”, *Crónica Jurídica Hispalense: revista de la Facultad de Derecho*, n. 22, 2024, pp. 180-211

<https://hdl.handle.net/11441/175663>).

García Torres, M. L., “La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal”, *Ciencia Policial*, vol. 183, 2024, pp. 91-132 (<https://doi.org/10.14201/cp.32177>).

Gimeno Beviá, J., “Policía y justicia predictiva en España: análisis actual y reflexión crítica” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, pp. 139-166.

González Álvarez, J. L., López-Ossorio, J. J., Urruela, C., Rodríguez-Díaz, M., “Integral Monitoring System in Cases of Gender Violence VioGén System”, *Behavior & Law Journal*, vol. 4, n. 1, 2018, pp. 29-40 (<https://doi.org/10.47442/blj.v4.i1.56>).

Marchena Gómez, M., “Inteligencia artificial y jurisdicción penal”, *Real Academia de Doctores de España*, 2022, pp. 1-98.

Martínez Garay, L., “Peligrosidad, algoritmos y due process: el caso State v. Loomis”, *Revista de Derecho Penal y Criminología*, n. 20, 3ª época, 2020, pp. 485-502 (<https://doi.org/10.5944/rdpc.20.2018.26484>).

Martínez Garay, L., “Tres sistemas de policía predictiva en España: VIOGÉN, RISCANVI y VERIPOL: Evaluación desde una perspectiva de derechos humanos”, *Publicacions De La Universitat De València*, 2026 (<https://doi.org/10.7203/PUV-OA-9788411186605>).

Montesinos García, A., “Inteligencia artificial en la justicia con perspectiva de género: amenazas y oportunidades”, *Actualidad Jurídica Iberoamericana*, n. 21, 2024, pp. 566-597.

Muñoz Aranguren, A., “¿Derecho a una decisión humana? El uso de la inteligencia artificial en la predicción judicial de la reincidencia”, *Anuario Jurídico Secciones ICAM Sepin Colex*, 2021.

Neira Pena, A. M., “Inteligencia artificial y tutela cautelar. Especial referencia a la prisión provisional”, *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 3, 2021, pp. 1897-1993 (<https://doi.org/10.22197/rbdpp.v7i3.618>).

Oliveira, L., Tavares, C., Strzelecki, A., Silva, M., “Prompting Minds: Evaluating How Students Perceive Generative AI's Critical Thinking Dispositions”, *Electronic*

Journal of E-learning, vol. 23, n. 1, 2025
(<https://doi.org/10.34190/ejel.23.2.3986>).

Pereira Puigvert, S., “La justicia y el proceso penal en clave algorítmica. Nuevos enfoques, nuevos riesgos”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, pp. 66-79
(<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.03>).

Rangugni, M. C., “Inteligencia Artificial en las sentencias de la justicia criminal” en De Luca, J. A., Ramos, M. A. (dirs.), Figueroa, F., Kleiman, H., Parra M. (coords.), *Inteligencia artificial y Administración de justicia: la policía predictiva y la justicia predictiva*, Jusbaire, Buenos Aires, 2025, pp. 113-131.

Roa Avella, M. D. P., Sanabria-Moyano, J. E., Dinas-Hurtado, K., “Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos”, *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 1, 2022, pp. 275-310
(<https://doi.org/10.22197/rbdpp.v8i1.615>).

Sánchez Sáez, A. J., “El posible uso de la inteligencia artificial en el ámbito judicial: contexto jurídico español y europeo. Especial referencia al contencioso-administrativo”, *Rivista italiana di informatica e diritto*, vol. 5, n. 2, 2023, pp. 163-200 (<https://doi.org/10.32091/RIID0118>).

Yáñez García-Bernalt, I., “La inteligencia artificial en el proceso penal: eficiencia versus garantías”, *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 10, n. 2, 2024, pp. 80-100 (<https://doi.org/10.12795/IESTSCIENTIA.2024.i02.04>).

4. RECURSOS DE INTERNET

Advancing Pretrial Policy & Research, “Pretrial Research Summary: The Public Safety Assessment”, *Advancing Pretrial Policy & Research (APPR)*, 2021 (disponible en <https://www.advancingpretrial.org/resource/research/>; última consulta 24/03/2026).

Anderson, C., Redcross, C., Valentine, E. y Miratrix, L., “Evaluation of Pretrial Justice System Reforms That Use the Public Safety Assessment: Effects of New Jersey’s Criminal Justice Reform”, *MDRC Center for Criminal Justice Research*, Report 1, 2019 (disponible en <https://www.mdrc.org/work/publications/evaluation-pretrial-justice-system-reforms-use-public-safety-assessment-0>; última consulta

24/03/2026).

Angwin, J., Larson, J., Mattu, S., Kirchner, L., “Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks”, *ProPublica*, 23 de mayo de 2016 (disponible en <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; última consulta 24/03/2026).

Arandia, P. J., Ley, M., Luengo, J., Martín, L., Mateo, M., Ortega, M. G., Siqués, S., “Un algoritmo define el futuro de los presos en Cataluña: ahora sabemos cómo funciona”, *El Confidencial*, 24 de abril de 2024 (disponible en https://www.elconfidencial.com/tecnologia/2024-04-24/riscanvi-algoritmo-cataluna-prisiones-presos-inteligencia-artificial_3871170/; última consulta 24/03/2026).

Big Brother Watch Team, “A Closer Look at Experian Big Data and Artificial Intelligence in Durham Police”, *Big Brother Watch*, 6 de abril de 2018 (disponible en <https://bigbrotherwatch.org.uk/blog/a-closer-look-at-experian-big-data-and-artificial-intelligence-in-durham-police/>; última consulta 24/03/2026).

Centro de Estudios Políticos y Constitucionales (CEPC), “Inteligencia artificial y justicia”, *Centro de Estudios Políticos y Constitucionales dependiente del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes*, 2025 (disponible en <https://www.cepc.gob.es/documentacion/informes-tematicos>; última consulta 24/03/2026).

Cuatrecasas Monforte, C., “La Inteligencia Artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos”, *Universitat Ramon Llull*, 2022 (disponible en <http://hdl.handle.net/10803/675100>; última consulta 24/03/2026).

García, T., Torrecillas, C., Maqueda, A., “La Policía Nacional deja de usar Veripol, su IA estrella para detectar denuncias falsas”, *El País*, 19 de marzo de 2025 (disponible en <https://elpais.com/tecnologia/2025-03-19/la-policia-nacional-deja-de-usar-veripol-su-ia-estrella-para-detectar-denuncias-falsas.html>; última consulta 24/03/2026).

Ministerio del Interior, “Interior diseña un nuevo modelo de respuesta policial a la violencia de género”, *La Moncloa: Web oficial del presidente del Gobierno y el Consejo de Ministros*, 15 de enero de 2025 (disponible en

<https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2025/150125-marlaska-redondo-sistema-viogen-2.aspx>; última consulta 24/03/2026).

Miranda, G., “Justicia algorítmica y medidas cautelares en el proceso penal. ¿Puede la IA solucionar los problemas de la decisión sobre la prisión provisional?”, *Castellarnau Penalistas*, 26 de septiembre de 2023 (disponible en <https://www.castellarnaupenalistas.com/>; última consulta 24/03/2026).

Policía Nacional, “La Policía Nacional pone en funcionamiento la aplicación informática VeriPol para detectar denuncias falsas”, *Portal web de la Policía Nacional*, 27 de octubre de 2018 (disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=4433&idioma_Actual=es#; última consulta 24/03/2026).

Redacción Lefebvre, “Medidas cautelares en el proceso penal”, *El Derecho*, 1 de septiembre de 2023 (disponible en <https://elderecho.com/medidas-cautelares-en-proceso-penal>; última consulta 24/03/2026).

Rubio, I., “Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres”, *El País*, 12 de octubre de 2018 (disponible en https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html; última consulta 24/03/2026).