

Ética, Derecho y percepción de la Justicia en el entorno digital europeo, con especial referencia al Reglamento de IA

Ethics, Law and perception of Justice in the European digital environment, with special reference to AI Regulation

CARMEN JEREZ DELGADO*
Catedrática de Derecho civil
Universidad Autónoma de Madrid

Recibido: 21.01.2026 / Aceptado: 11.02.2026

DOI: 10.20318/cdt.2026.10277

Resumen: Este trabajo analiza el uso de la IA por jueces y magistrados europeos desde la perspectiva jurídica, especialmente marcada por el Reglamento (UE) 2024/1689, sin prescindir de aspectos conexos. Al tiempo de su entrega a la revista CDT, se ha publicado en España la Instrucción 2/2026, del Consejo General del Poder Judicial, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional (BOE núm. 27 de 30 enero 2026), que viene a corroborar lo que aquí se explica, y que ha sido incorporada al texto.

Palabras clave: Reglamento (UE) 2024/1689, jueces y magistrados, abuso de la IA, responsabilidad, Instrucción 2/2026 del Consejo General del Poder Judicial.

Abstract: This paper deals with the use of AI by judges and magistrates from a legal perspective, particularly marked by the Regulation (EU) 2024/1689, without neglecting related aspects. At the time of submission to the publisher, Instruction 2/2026 of the Spanish General Council of the Judiciary on the use of artificial intelligence systems in the exercise of judicial activity (BOE núm. 27, January 30, 2026) was published, corroborating what is explained here, and has been incorporated into the text.

Keywords: Regulation (EU) 2024/1689, judges and magistrates, abuse of AI, liability, Instruction 2/2026 of the Spanish General Council of the Judiciary.

Sumario: I. Planteamiento. II. Perspectiva ética. III. Perspectiva jurídica. 1. El uso de la IA por la autoridad judicial. A) Las prácticas prohibidas y sus excepciones. B) Los usos admitidos y la distinción de los sistemas de alto riesgo. a) Los usos admitidos en el panorama nacional. b) Los sistemas de alto riesgo conforme al Reglamento IA: La alusión a jueces y magistrados. 2. Requisitos de los sistemas de IA de alto riesgo. A) La supervisión humana. B) La transparencia. C) La trazabilidad. 3. La responsabilidad por el abuso de los sistemas de IA de alto riesgo. IV. Perspectivas sociológica y psicológica, a modo de corolario. V. Conclusiones.

*Investigadora principal del proyecto “Hacia un Derecho procesal de consumo: un paso en la modernización de la jurisdicción civil en el contexto europeo” (PID 2020-117624GB-I00). carmen.jerez@uam.es .

I. Planteamiento

1. La cuestión que planteo aquí es la relativa al uso de la inteligencia artificial (IA) por los jueces y juezas, magistrados y magistradas (en adelante, jueces y magistrados) europeos en el desempeño de sus funciones, y quisiera hacerlo en un tono reflexivo, jurídico-técnico pero abierto al debate, y que toma como referencia necesaria el Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia 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 (DOUE de 12 julio 2024; *Reglamento de Inteligencia Artificial*, en adelante, Reglamento IA en el texto, o RIA cuando acompañe a la referencia a un artículo).

El uso de la inteligencia artificial por jueces y magistrados europeos pone en jaque -se ha dicho- al sistema de reconocimiento mutuo de sentencias en el Espacio Judicial Europeo¹: ¿Se hace de verdad necesario estandarizar los sistemas de IA empleados en este ámbito a fin de solventar las dificultades que pueden presentarse para ese reconocimiento mutuo? La realización del presente estudio me permite opinar sobre la cuestión: Si se siguen las reglas del Reglamento IA, los criterios de transparencia y trazabilidad estarían armonizados; como lo estaría también la necesidad de supervisión humana, con tal que al menos un juez o magistrado (o un mínimo de dos, si se tratasen datos biométricos) la llevase a cabo; pero quizás sí sería muy aconsejable estandarizar los sistemas de IA que puede emplear un juez o magistrado europeo como apoyo para el desempeño de su función jurisdiccional².

En España, este último aspecto ha sido abordado en parte por la Instrucción 2/2026, del Consejo General del Poder Judicial, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional (BOE núm. 27 de 30 enero 2026)³, al limitar estos sistemas a los facilitados por el CGPJ o la Administración competente (en adelante, Instrucción CGPJ)⁴.

Más allá del Espacio Europeo de Justicia, sí resulta del todo necesario, a mi juicio, acordar estándares en todos los aspectos citados (transparencia, trazabilidad, supervisión humana, sistemas de IA empleados), a fin de alcanzar la deseada seguridad jurídica a la hora de aplicar convenios internacionales relativos al reconocimiento de decisiones judiciales, tales como -en materia civil y mercantil- el

¹ Como es sabido, el reconocimiento y ejecución de resoluciones mercantiles y civiles en el entorno europeo, está regulado por el Reglamento (UE) n° 1215/2012, del Parlamento europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DOUE de 20 diciembre 2012), que mantiene la lógica de reconocimiento mutuo de resoluciones judiciales y coordinación interjurisdiccional del Convenio de Bruselas de 1968, relativo a la competencia judicial y la ejecución de resoluciones judiciales en materia civil y mercantil (Diario Oficial n° C 027 de 26/01/1998 p. 0001-0027), del que puede decirse que sentó las bases para la cooperación judicial en el espacio europeo. ¿Se alteran estas bases cuando un juez hubiera empleado un sistema de IA como ayuda en el desempeño de la función jurisdiccional? A juicio de A.M. LÓPEZ RODRÍGUEZ («Eficacia transfronteriza de decisiones judiciales asistidas por inteligencia artificial en el Espacio Judicial Europeo», *Cuadernos de Derecho Transnacional*, octubre 2025, Vol. 17, N° 2, pp. 437-454, p. 454), se hace necesario estandarizar a nivel europeo criterios sobre la transparencia, la supervisión humana, o los sistemas de IA utilizados por jueces y magistrados, a fin de dotar de seguridad jurídica al espacio judicial de la UE. La autora explica que *la convergencia regulatoria* de aspectos tales como la transparencia, las reglas de protección de datos, o la supervisión humana, con ocasión del Reglamento IA o del *Convenio Marco del Consejo de Europa*, viene a facilitar *la interoperabilidad de los sistemas de IA entre jurisdicciones* (p. 451). Por esta razón, a su juicio, *los instrumentos existentes en materia de Derecho internacional privado deben tomar como referencia tanto el RIA como el Convenio Marco del Consejo de Europa sobre inteligencia artificial*; y señala como ejemplo las Reglas Modelo europeas de Proceso civil ELI/UNIDROIT (pp. 452-453).

² El proceso pudiera ir de la mano (aunque no necesariamente) del que se hace necesario para implementar el Reglamento (UE) 2023/2844, del Parlamento europeo y del Consejo, de 13 de diciembre de 2023, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial (DOUE del 27 diciembre 2023), abordado en el V Foro europeo de Derecho internacional privado (al respecto, puede verse la obra colectiva *Digitalización, inteligencia artificial y Derecho internacional privado* coordinada por A.FERNÁNDEZ PÉREZ, Aranzadi-La Ley, 2025; en particular, los dos capítulos autoría de la coordinadora de la obra).

³ Aplicable desde la fecha de su publicación en el BOE (ordinal Decimocuarto de la Instrucción CGPJ).

⁴ Agradezco a la coordinadora de la revista CDT, Isabel Antón Juárez, y a su director, Alfonso Calvo Caravaca, la amabilidad de permitirme actualizar el texto en fecha tan avanzada (30 enero 2026).

denominado nuevo Convenio de Lugano (2007)⁵, o el Convenio de La Haya (2019)⁶. Más aún habida cuenta de las disparidades normativas y tecnológicas existentes entre los diversos países⁷. Espero que este artículo, relativo al uso de la IA por jueces y magistrados europeos conforme a lo dispuesto en el Reglamento IA, contribuya a que el lector se forme una opinión sobre la cuestión planteada, como a la autora le ha sucedido al escribirlo.

2. Para delimitar el alcance de la materia que vamos a tratar, conviene precisar que la definición de la IA en el Reglamento citado abarca sólo los sistemas diseñados para funcionar con cierta autonomía, de modo que a partir de las fuentes de información que se les suministren como punto de partida (*input*), pueden producir resultados (*output*) tales como *predicciones, contenidos, recomendaciones o decisiones* adaptados al caso [artículo 3.1) RIA]. Por tanto, quedan excluidos de nuestra consideración específica, aunque podamos hacer alguna alusión ocasional a ellos, los sistemas basados en la programación informática tradicional o tecnologías para la realización de operaciones automáticas⁸.

3. La característica clave de los sistemas de IA regulados por el Reglamento consiste en su *capacidad de inferencia*, es decir, de alcanzar resultados a partir de la información o los datos de entrada. Aunque la capacidad de inferencia propia de los sistemas de IA objeto de nuestro estudio, se define en términos que por analogía podemos comprender, tales como que estas máquinas pueden desarrollar *estrategias de aprendizaje automático, y estrategias basadas en la lógica*⁹, conviene recordar que sería un craso error identificarlas con la mente humana, pues estos sistemas sólo cuentan con las fuentes de datos que se les suministran, y carecen tanto de la conciencia como de la flexibilidad y las capacidades de ponderación y proyección que tiene el ser humano.

En concreto, a efectos de elaborar el borrador de una sentencia, hay que tener en cuenta que un sistema de IA no tiene juicio propio, sino que extraerá resultados a partir -a lo más- de juicios ajenos sobre casos semejantes al que se trate. Estos juicios ajenos serán el único elemento con el que cuenta para *interpretar* las normas aplicables. Nuevamente empleo una palabra (*interpretar*) que sirva para entendernos, pero sólo se trata de una analogía, pues la IA no puede aplicar los criterios hermenéuticos del artículo 3 del Código civil (por ejemplo, no puede dar solución a una situación sin precedentes conectando el sentido propio de las palabras de las normas existentes con la realidad social del tiempo en que han de ser aplicadas)¹⁰.

⁵ Decisión del Consejo de 15 octubre 2007 relativa a la firma, en nombre de la Comunidad, del Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (2007/712/CE); DOUE del 21 diciembre 2007.

⁶ Convención de 2 de julio de 2019 sobre el Reconocimiento y la Ejecución de Sentencias Extranjeras en Materia Civil y Comercial (entrada en vigor el 1 septiembre 2023).

⁷ Una visión panorámica autorizada sobre la diversidad legislativa en el ámbito internacional y la escasa jurisprudencia relacionada hasta el momento es la ofrecida por el Centro de Estudios Políticos y Constitucionales, en el Dossier *Inteligencia artificial y Justicia* (Servicio de Documentación Jurídica, Subdirección General de Publicaciones y Documentación, septiembre 2025). Como ha explicado A.M. LÓPEZ RODRÍGUEZ («Eficacia transfronteriza de decisiones judiciales asistidas por inteligencia artificial en el Espacio Judicial Europeo», *Cuadernos de Derecho Transnacional*, octubre 2025, Vol. 17, N° 2, pp. 437-454, p. 444), *las resoluciones dictadas -por ejemplo- por los tribunales automatizados chinos podrían motivar el rechazo por parte de otros países con regulaciones más estrictas*.

⁸ Se insiste en esta diferenciación en el considerando (12) RIA.

⁹ Expresiones tomadas del considerando (12) RIA. El legislador europeo afirma en este considerando que la citada capacidad de inferencia de los sistemas de IA *trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización*. Sin embargo, hemos de recordar que este razonamiento se atiene a las estrictas reglas de la lógica, mientras el razonamiento humano está enriquecido con la intuición, la abstracción, la analogía, la verificación de las premisas, o la posibilidad de proyección. En su condición de experto, Moisés BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, p. 21], define la inferencia como un *proceso mediante el cual el sistema utiliza la información disponible para deducir o calcular un resultado, basándose en modelos, algoritmos o reglas establecidos en la fase previa de entrenamiento o construcción*.

¹⁰ Como indica A. PERALTA GUTIÉRREZ («Impacto comparado de la IA en la Administración de Justicia», en *La GuIA práctica de inteligencia artificial*, n° 5, noviembre 2025, Aranzadi-La Ley, pp. 1-30, p. 30), la IA aporta *soluciones lógicas*, pero *no garantiza la justicia humana*. Por esta razón, a su juicio, la IA sirve como apoyo a la actividad judicial y puede mejorar la productividad, lo que no puede hacer es *sustituir el componente humano esencial*.

4. Los puntos de los que parto para reflexionar sobre el uso por jueces y magistrados de estos sistemas de IA son las perspectivas ética y -principalmente- jurídica, sin dejar de atender a factores de otra índole que influyen en nuestro modo de percibir la justicia cuando nos movemos en el entorno digital y que están presentes tanto en el debate teórico como en la actuación práctica, que -en última instancia- es lo que nos afecta, sea como operadores jurídicos, sea como destinatarios del trabajo de los operadores jurídicos.

II. Perspectiva ética

5. Desde la perspectiva ética, el buen juez se define como aquél que es independiente, imparcial, íntegro, prudente, formado (conoce el Derecho), responsable y con dedicación al desempeño de su función, como quien sirve¹¹. ¿Qué uso de la IA por parte de jueces y magistrados es compatible con esta definición?

6. El pasado 8 de octubre, celebramos en la Facultad de Derecho de la Universidad Autónoma de Madrid el Seminario de profesores titulado *Los Principios de ética judicial a examen: IA y Administración de Justicia*, donde la que fuera miembro experto de la Comisión de ética judicial del Consejo General del Poder Judicial, la Catedrática de Filosofía del Derecho Cristina Hermida del Llano, nos ilustró sobre las cuestiones que plantea el uso de la IA por jueces y tribunales desde una perspectiva ética.

Partiendo de la base de que la persona humana ha de estar *en el centro*, como pieza esencial y más importante de cualquier reflexión o normativa en la materia, nuestra ponente comenzó y concluyó su exposición con sendas preguntas: Cuestionó al inicio si el uso de la IA en este contexto nos permite vivir mejor, salvaguardando siempre los derechos fundamentales, y concluyó dejando en el aire el interrogante de si terminaremos los seres humanos amando nuestro propio sometimiento a las máquinas.

A juicio de Cristina Hermida del Llano, el poder tecnológico no sólo amenaza con romper el equilibrio de los tres poderes constitucionales, sino la imparcialidad, la independencia y la integridad de los jueces. Dicho de otro modo, amenaza con desnaturalizar la esencia del poder judicial¹². Por esta razón, entre otras, es necesaria una regulación legal que garantice un uso de la IA por parte de la Administración de Justicia acorde con el interés general y, por consiguiente, con los derechos fundamentales de la persona. Un uso indebido de la IA en este ámbito -explicó- haría peligrar la confianza de la ciudadanía en la justicia, cuando precisamente está en la base del poder judicial incrementar siempre esa confianza.

7. Parece claro que la reflexión ética exige que la persona humana (y su entorno natural) constituya el valor por excelencia de toda regulación de la materia. Si damos un paso hacia la perspectiva jurídica, el criterio no puede ser distinto, toda vez que los textos constitucionales y los tratados europeos e internacionales en materia de derechos humanos suponen un claro imperativo que debe ser respetado por cualquier otra norma, y que por tanto viene a delimitarla sea expresa o implícitamente.

¿Cuál es el caso, cuando nos referimos al principal texto normativo que hoy rige la materia, esto es, al citado Reglamento europeo de inteligencia artificial¹³?

¹¹ I. SANCHO GARGALLO, «Ética judicial. El paradigma del buen Juez», *ICADE, Revista de la Facultad de Derecho*, núm. 72, 2007, pp. 117-138, p. 121. Juan DAMIÁN MORENO [«¿En qué consiste ser un buen juez?»], en *Justicia restaurativa: una justicia para las víctimas*, Soletto Muñoz/Carrascosa Miguel (codirs.), 2019, Tirant lo Blanch, pp. 227-236, pp. 235-236] ha insistido en que si bien es importante la integridad de los jueces, lo determinante para garantizar que la decisión es conforme a la ley es su formación, y el fomento de la excelencia profesional.

¹² En este sentido se ha pronunciado la Comisión Iberoamericana de Ética Judicial (CIEJ), en su Dictamen *sobre el uso ético de la inteligencia artificial en la labor jurisdiccional* (8 de septiembre de 2023). En concreto, el texto se refiere al análisis jurídico y probatorio de casos concretos, afirmando que, si la IA sustituyera plenamente las decisiones humanas en ese ámbito, *se desnaturalizaría el sistema judicial de inspiración democrática*. Y se argumenta sobre el carácter imprescindible del criterio humano en cuestiones que pueden ser *novedosas*, o que implican *zonas grises*, en relación con las que los jueces desempeñan una función de impulso al desarrollo, evolución y adaptación a las necesidades de una sociedad concreta (núm. 43).

¹³ Si bien el Reglamento IA no ha sido el primer texto jurídico en la materia, sí constituye el marco de referencia actual para la gobernanza de la inteligencia artificial.

El Reglamento IA pretende cumplir este imperativo ético, toda vez que en sus primeros considerandos, junto a una declaración general de las ventajas económicas y sociales del desarrollo de la IA (referidas entre otros sectores al ámbito de la justicia)¹⁴, y a una declaración general de la consciencia del legislador de los riesgos que supone esta tecnología -entre los que se encuentra el de *menoscabar los intereses públicos y los derechos fundamentales* amparados por el derecho de la UE-¹⁵, encontramos una tercera declaración general del carácter esencial que tiene que el Reglamento se desarrolle conforme a los valores, derechos y libertades fundamentales reconocidos por el derecho de la UE¹⁶. En el considerando (6) del Reglamento IA, se afirma expresamente que *la IA debe ser una tecnología centrada en el ser humano*; que la IA debe ser una *herramienta para las personas*; y que el objetivo último de la IA debe ser *aumentar el bienestar humano*.

Es más, la centralidad de la persona humana se refleja en el artículo 1 del Reglamento IA, al definir su objeto como la mejora del mercado interior y la promoción de una IA *centrada en el ser humano y fiable*. Por consiguiente, si bien no es el primer objetivo del legislador afirmar la centralidad de la persona humana, sí se tiene en cuenta su primacía, en relación con el tipo de IA que se quiere promover junto a la mejora del funcionamiento del mercado de la UE. Además, existen numerosas delimitaciones estratégicamente ubicadas al final de determinados artículos del Reglamento IA (como sucede también en este primero), que garantizan la protección y el respeto por la salud, la seguridad y los derechos fundamentales de la persona, así como por la democracia, el Estado de Derecho, y el medio ambiente. Esta característica del Reglamento pone de relieve, a su vez, que el legislador es muy consciente de que el uso de la IA no es inocuo, sino que constituye un riesgo para los derechos, instituciones y valores citados, que le mueve a tomar medidas severas que afectan tanto a los *proveedores*¹⁷ de sistemas de IA, como a los profesionales usuarios de los mismos, denominados *responsables del despliegue*^{18, 19}.

En otros textos europeos encontramos también declaraciones expresas en este sentido. Por ejemplo, el Consejo de Europa ha consensuado un convenio en materia de IA con el objetivo de garantizar que las actividades realizadas contando con la IA sean plenamente respetuosas con los derechos humanos, la democracia y el Estado de derecho²⁰, y -por otra parte- el Parlamento Europeo, en su Resolución de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital ha declarado que *la IA debe ser una tecnología centrada en el ser humano y fiable*²¹. Previamente, el Consejo de Europa había acordado los

¹⁴ Considerando (4) RIA. A ello contribuyen las Directrices (2019) del Grupo independiente de expertos de alto nivel sobre IA, a que alude el legislador en el Considerando (27) RIA.

¹⁵ Considerando (5) RIA.

¹⁶ Considerando (6) RIA. Volvemos a encontrar declaraciones de intenciones en este sentido constantemente. Por ejemplo, en los Considerandos (8-10) RIA, que incluyen referencias especiales al derecho fundamental a la protección de datos personales.

¹⁷ Se define como proveedor en el Reglamento de IA a la *persona física o jurídica, autoridad pública, órgano u organismo* que desarrolle o para quien se desarrolle *un sistema de IA o un modelo de IA de uso general* y lo ponga en servicio o introduzca en el mercado con su propia marca o nombre, sea gratuitamente o a cambio de un precio [artículo 3.3) RIA].

¹⁸ El Reglamento de IA define como responsable del despliegue a la *persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad* y en el marco de una actividad profesional (artículo 3.4 RIA). Moisés BARRIO ANDRÉS («Los sujetos obligados en el Reglamento UE de inteligencia artificial», *Cuadernos de Derecho Transnacional*, octubre 2025, Vol. 17, N° 2, pp. 69-79, p. 73) explica que los usuarios de IA que son denominados *juridicamente como responsables del despliegue, son actores que utilizan un sistema de IA "bajo su autoridad", lo que debe interpretarse como el ejercicio de cierto grado de control sobre el sistema*.

¹⁹ Las obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo (artículo 26 RIA coinciden en parte, pero no en todo, con las obligaciones de los proveedores (importadores y distribuidores incluidos). Estas últimas son más exigentes (artículos 16 y 25 RIA, y artículos intermedios, en particular, 22-24).

²⁰ *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS N° 225, Vilnius, 5.IX.2024, Artículo 1. Este convenio no entrará en vigor hasta que haya sido ratificado por cinco Estados, de los cuales al menos tres sean miembros del Consejo de Europa.

²¹ Con estas palabras se declara la centralidad de la persona humana en el punto (7) de la Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)), entre otros (por ejemplo, en los puntos número 117, 137, 224, o 265). En su introducción (1) se explica que el Parlamento Europeo *hace hincapié en que se ha de configurar la transformación digital dentro del pleno respeto de los derechos fundamentales* y de modo que la tecnología digital esté al servicio de la humanidad. La Resolución citada tuvo en cuenta la Comunicación de la Comisión, de 8 de abril de 2019, titulada *Generar confianza en la inteligencia artificial centrada en el ser humano* (COM(2019)0168).

principios que sirven como punto de partida en relación con el uso de la IA, dirigidos todos a garantizar la primacía de la protección de la persona y sus derechos fundamentales²².

En sentido semejante, en el considerando (27) del Reglamento IA se alude a los siete principios enunciados como *Directrices éticas* por el Grupo independiente de expertos de alto nivel sobre IA²³. Aunque se trata de principios no vinculantes, tienen por finalidad impulsar tanto la fiabilidad como el *fundamento ético de la IA*. Por su alusión a la ética y porque el legislador del Reglamento IA insta a todos los interesados a que tengan en cuenta estos principios éticos, conviene citarlos aquí. Son los siguientes:

- 1º El principio de *acción y supervisión humanas*, que pretende garantizar el respeto por la dignidad humana.
- 2º El principio de *solidez técnica y seguridad*, que busca reducir en lo posible los daños que pudieran generarse por el uso de los sistemas de IA.
- 3º El principio de *gestión de la privacidad y de los datos*, que alude a que toda actividad debe realizarse en consonancia con la normativa europea de protección de la intimidad y los datos personales.
- 4º El principio de *transparencia*, que se enuncia en el doble sentido de que el sistema facilite la trazabilidad para dar explicación de los procesos seguidos, a la vez que garantice que tanto el usuario profesional del sistema o responsable del despliegue sea consciente de las características y límites del sistema de IA con el que interactúa, como que el tercero que pueda resultar afectado conozca sus derechos.
- 5º El principio de *diversidad, no discriminación y equidad*, cualidades referidas tanto a los agentes de los sistemas de IA, como a los terceros afectados por los resultados del uso de dichos sistemas.
- 6º El principio de *bienestar social y ambiental*, que no sólo alude al respeto al medio ambiente y a la sostenibilidad, sino también -nuevamente- al cuidado de la persona, de la sociedad y de la democracia.
- 7º El principio de *rendición de cuentas*, relacionado el de transparencia.

8. En cuanto a la función judicial, ante el carácter todavía difuso de las reglas del juego, y a la vista de los riesgos que se asumen pero también de las ventajas que los sistemas de IA pueden reportar para el desempeño de las tareas que le son propias, es normal que se demande una normativa sectorial²⁴ que garantice *la justicia en un entorno de creciente automatización*, con la debida definición de la responsabilidad de los *actores involucrados*²⁵, y la necesaria diferenciación de tareas en las que la IA puede servir de apoyo o soporte en el ámbito de la Administración de Justicia. Esta demanda ha sido en parte atendida por la citada Instrucción CGPJ que, tomando como referencia tanto el Reglamento IA como

²² Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno (Comisión europea para la eficiencia de la justicia, CEPEJ), Estrasburgo, 3-4 de diciembre de 2018 [CEPEJ (2018) 14]. El texto enumera los siguientes principios: (1º) El principio de respeto de los derechos fundamentales; (2º) el principio de no discriminación; (3º) el principio de calidad y seguridad; (4º) el principio de transparencia, imparcialidad y equidad; (5º) el principio conforme al cual los resultados o las decisiones han de estar bajo el control del usuario. A la luz de este texto y de los antes citados, se puede concluir -con Encarnación ABAD ARENAS («La utilización de la inteligencia artificial en el sistema judicial: Marco ético», en *Inteligencia artificial y protección de datos. Desafíos en la era digital*, Colex, 2025, pp. 41-71)- que los principios éticos por los que debe regirse el uso de la inteligencia artificial en el ámbito jurídico *encuentran su razón de ser* en el respeto de los derechos fundamentales y en la autonomía y dignidad de las personas (p. 66).

²³ *Ethics Guidelines for Trustworthy AI* (2019). El Grupo de expertos independientes se estableció por la Comisión Europea en 2018.

²⁴ F. ZUIDERBEEN BORGESIU, «Discrimination, artificial intelligence, and algorithmic decision-making», publicado por el Consejo de Europa (Dirección General para la democracia, 2018). El autor explica que una regulación generalista no es suficiente, porque las cuestiones que surgen en cada sector son distintas. A su juicio, se requiere más debate e investigación multidisciplinar (p. 73).

²⁵ VV.AA., «Ética y responsabilidad en el uso de la IA en procesos judiciales», en *Verdad y Derecho. Revista arbitrada de ciencias jurídicas y sociales*, volumen 3 (especial 2), 2024, pp. 239-246, conclusiones.

la Política de uso de la inteligencia artificial en la Administración de Justicia²⁶, parte de los principios de control humano efectivo; no sustitución de los jueces y magistrados; responsabilidad judicial; independencia judicial; respeto a los derechos fundamentales; confidencialidad y seguridad; prevención de sesgos algorítmicos; proporcionalidad y uso limitado; y, por último, formación y capacitación²⁷.

Desde el punto de vista ético, no es lo mismo el uso de un sistema de IA en una oficina judicial para la compilación de datos o la programación de audiencias, que el uso de un sistema de IA para tomar decisiones de modo autónomo. Esta última función debe vetarse a la IA, ya que afecta a los derechos fundamentales de la persona y habida cuenta de que los sistemas de IA no tienen capacidad para emitir una valoración moral, ni pueden *comprender el contexto emocional o psicológico de una situación concreta*, ni interpretar el espíritu de la norma, que son aspectos inherentes a la función jurisdiccional, en cuyo desempeño el juez goza del *margen de discrecionalidad*²⁸. En este sentido, se ha recordado que la IA no sólo es una inteligencia sin ética ni conciencia, sino que está sujeta a hackeos, errores, desfases y sesgos²⁹.

III. Perspectiva jurídica

9. *En consonancia con la presunción de inocencia, las personas físicas de la Unión siempre deben ser juzgadas basándose en su comportamiento real. Las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles (...).*

Esta cita del considerando (42) del Reglamento IA atrae nuestra atención sobre un ejemplo gráfico de los riesgos que los sistemas de IA pueden suponer para las personas en el ámbito de la Administración de Justicia, según el uso que de ellos se haga.

10. Con la publicación del Reglamento IA de 2024 que -como indiqué al inicio- será el marco jurídico de la materia objeto de estudio, el legislador de la Unión ha tomado medidas precisas y directamente aplicables, dirigidas a la protección de las personas ubicadas en la UE ante el uso de sistemas avanzados de IA con carácter general, que obligan a proveedores y responsables del despliegue de sistemas de IA establecidos en la UE o cuyos resultados se utilicen en la UE³⁰. Y lo hace con una doble distinción, en función del *riesgo*³¹ que implique el uso al que se destinen: De un lado, distingue entre sistemas de IA prohibidos (artículo 5 RIA) y los restantes sistemas, cuyo uso está permitido (artículo 5 RIA, *a contrario sensu*, y artículos 6 y siguientes RIA); y, de otro lado, dentro de los sistemas cuyo uso se permite, el legislador europeo distingue -según el riesgo que ese uso supone-, entre los que son de alto riesgo (artículo 6 RIA), para los que exige notables requisitos (artículos 8-15 RIA), y los que no lo son (artículo 6 RIA, *a contrario sensu*; y artículos 51 y siguientes RIA).

En relación con la materia objeto de estudio, se consideran sistemas de alto riesgo -sin género de duda- aquéllos capaces de proporcionar el borrador de una resolución judicial, cuyo uso estaría pro-

²⁶ Publicada por la Secretaría General del Comité Técnico Estatal de la Administración Judicial Electrónica en junio de 2024.

²⁷ Ordinal Cuarto de la Instrucción CGPJ.

²⁸ Parafraseando aquí el Dictamen del CIEJ *sobre el uso ético de la inteligencia artificial en la labor jurisdiccional* (2023), núms. 11, 40 y 53. El Dictamen recomienda que se excluyan los usos de IA, en el ámbito de la función jurisdiccional, relativos a *razonamientos complejos*, o a la *ponderación en las decisiones judiciales*, así como la predicción de resultados o la determinación de probabilidades de que una persona vuelva a delinquir, mientras que recomienda su uso para *tareas repetitivas* relativas a formularios, cumplimiento de requisitos, y otras gestiones de esta índole (núm. 54).

²⁹ M. DE ASÍS PULIDO, «Ética de la Inteligencia Artificial jurídica aplicada al proceso», *Cuadernos electrónicos de Filosofía del Derecho*, núm. 48, 2023, pp. 60-79, p. 64. Inspirándose en textos de *soft law* existentes al tiempo de la publicación, el autor propone los siguientes principios éticos de la IA aplicada al proceso judicial: La no discriminación; la protección y calidad de los datos; la precisión, solidez y seguridad del sistema; la transparencia de los algoritmos; la imparcialidad del sistema (que no existirá cuando el uso del mismo implique el recurso por la IA a datos sesgados); la colaboración del jurista-técnico en el diseño de los sistemas; y, por último, el control humano del sistema.

³⁰ El Reglamento de IA protege a las personas ubicadas en la UE que puedan resultar afectadas por el uso de sistemas de IA [artículo 2.1.g) RIA]. En cuanto a los sujetos obligados, véase el artículo 2 RIA.

³¹ Como ha expresado Moisés BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*], Francis Lefebvre, 2025, p. 38, 180], *el RIA sigue un paradigma regulador basado en el riesgo*.

hibido si no mediase intervención humana para modificar y/o validar los resultados; mientras que se consideran dentro del grupo restante los dirigidos a *interactuar* con personas físicas (los denominados *chatbots*), o los sistemas correctores de textos, entre otros³². Más adelante profundizamos en ello. Antes quisiera matizar que, en relación con la panorámica general presentada de distinción entre sistemas prohibidos, sistemas de alto riesgo y el resto de los sistemas, ni una ni otra diferenciación quedan nítidamente definidas en el Reglamento de IA, como el blanco se distingue del negro, sino que hay margen para los grises:

En primer lugar, el artículo 5 RIA, enumera las prácticas de IA prohibidas, pero lo hace no al estilo *numerus clausus*, sino *numerus apertus*, ya que en su último párrafo (el número octavo) incluye las *prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión*. Lógicamente, bajo esta disposición pueden entenderse prohibidas todas las prácticas que infrinjan cualesquiera derechos fundamentales y garantías amparados por el Derecho de la Unión.

En segundo lugar, al establecer los criterios de clasificación de los sistemas de alto riesgo, el legislador deja constancia de varias incertidumbres que sólo la práctica llegará a aclarar: Muestra de ello es que se legitime expresamente a la Comisión para modificar lo establecido *cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales* (artículo 6.7 RIA, como también artículo 7 RIA, ambos relativos a los sistemas de alto riesgo descritos en el anexo III RIA). Esta apertura a futuras modificaciones conforme a lo que la experiencia vaya aconsejando es positiva, a mi juicio, y conecta directamente con la materia objeto de estudio pues -entre los sistemas de IA a los que se refiere el anexo III RIA- se encuentran los destinados a determinados usos que puede hacer la Administración de Justicia, según veremos a continuación.

11. Queda así de manifiesto tanto que el legislador es muy consciente de los riesgos que ciertos usos de la IA suponen para la persona humana, como que no quiere dar la espalda a las ventajas que su uso supone, de modo que apuesta por admitir el uso, pero adoptando medidas que garanticen del mejor modo la protección integral de las personas y la sociedad, cuando los derechos fundamentales están en riesgo³³. Así, la opción por el enfoque antropocéntrico, que constituye una intencionada aportación europea³⁴, lejos de frenar el avance tecnológico, implementa los sistemas de IA avanzada, con medidas de apoyo a la innovación (artículos 57-63 RIA), pero también con las debidas cautelas.

12. Veamos, en primer lugar, las normas jurídicas que -a nivel nacional y europeo- regulan el uso de los sistemas de IA por parte de la Administración de Justicia, determinando los contornos de lo admitido y lo prohibido. Y veamos después las medidas que el legislador europeo ha adoptado para garantizar la protección de los derechos fundamentales de la persona, cuando quedan expuestos a mayor riesgo, es decir, los anunciados requisitos que deben cumplir los sistemas de IA de alto riesgo para su puesta en circulación en el mercado europeo.

1. El uso de la IA por la autoridad judicial

13. Para abordar la cuestión del uso de la IA por jueces y magistrados desde una perspectiva jurídica debemos tener en cuenta, junto al Reglamento (UE) 2024/1689 sobre inteligencia artificial, la normativa nacional en la materia, incluyendo la citada Instrucción CGPJ y la Política de uso de la inteli-

³² A los *chatbots* se les aplica el régimen dispuesto en el artículo 50 RIA. Los *sistemas de bajo o nulo riesgo*, como el corrector de textos, no están regulados directamente en el RIA, aunque se haga alguna alusión a ellos [véase, al respecto, lo explicado por M. BARRIO ANDRÉS, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, p. 179, 1501].

³³ En este sentido, en el artículo 27 RIA se regula la obligación que pesa sobre entidades públicas y privadas que vayan a desplegar determinados sistemas de IA de alto riesgo, de evaluar el impacto del sistema en cuestión sobre los derechos fundamentales.

³⁴ Véase el punto 104 de la Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)).

gencia artificial en la Administración de Justicia, aprobada por el Pleno del Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE) el día 21 de junio de 2024³⁵. A diferencia de lo que hace el Reglamento europeo citado, que limita su ámbito a los sistemas de IA avanzada (capaces de cierta autonomía), la legislación española se refiere a un concepto amplio de IA que abarca también sistemas menos avanzados y automáticos³⁶.

Si atendemos a las funciones propias de la Administración de Justicia, comprobamos que para las más sencillas está ampliamente admitido en España el uso de sistemas de IA, mientras que para las más complejas, exclusivas de los jueces y magistrados, se toman más cautelas. En concreto, se admitirá que el juez o el magistrado se apoye en un sistema de IA para obtener el borrador de una posible sentencia, pero en ningún caso se admitirá que las sentencias o los autos judiciales se expidan de modo automático, es decir, sin la intervención humana. En España, los jueces y magistrados sólo pueden utilizar para el desempeño de la función jurisdiccional los sistemas de IA que la Administración competente en materia de Justicia, o el Consejo General del Poder Judicial, pongan a su disposición con esta finalidad [artículo Quinto (*Sistemas de IA permitidos en el ejercicio de la actividad jurisdiccional*), párrafo 1, Instrucción CGPJ]³⁷.

Junto a las tareas que ya tenemos asumido que realiza sin problemas un sistema de IA al servicio de la Administración de Justicia, tales como la anonimización de sentencias para su registro público a fin de preservar la privacidad con la debida protección de los datos personales, o bien el resumen de sentencias a fin de facilitar el conocimiento de su contenido en un menor lapso de tiempo³⁸, existen otras funciones que resultan más controvertidas. Por esta razón, en el panorama europeo encontramos prácticas prohibidas y sistemas de IA declarados de alto riesgo, para cuya puesta en circulación en el mercado deberá quedar garantizado el cumplimiento de notables requisitos.

A) Las prácticas prohibidas y sus excepciones

14. Ya hemos visto que el artículo 5 del Reglamento IA enumera las prácticas de IA prohibidas, y lo hace con la técnica del *numerus apertus*, dejando en su último apartado una prohibición general de cualquier uso contrario al Derecho de la Unión: El legislador blindo así la seguridad y los derechos fundamentales de las personas con tuerca y contratuerca (artículo 5.8 RIA). Al conectar esta regla general con la función de los jueces y magistrados, parece claro que, entre los derechos fundamentales de las personas que pudieran quedar afectadas por un sistema de IA que expidiera de modo automático autos o sentencias de carácter ejecutivo se contarían los derechos a la seguridad jurídica (artículo 9 CE) y a la tutela judicial efectiva (artículo 24 CE). Por esta razón, se prohíbe un sistema de estas características: *La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe sustituirlas: la toma de decisiones finales debe seguir siendo una actividad humana* [Considerando (61) RIA]³⁹.

³⁵ Como antes se indicó, este último documento ha sido tenido en cuenta por la Instrucción CGPJ de 28 de enero de 2026 (BOE núm. 27 de 30 enero 2026) sobre la materia, por lo que muchos de sus aspectos quedan subsumidos en la Instrucción. No obstante, cabe destacar que el CTEAJE presenta en el texto citado (Anexo II) un cuadro indicativo de *usos permitidos y prohibidos*, en el que se especifican las autoridades que deben ser consultadas a efectos de obtener la autorización requerida para determinados usos, conforme a la política aprobada por este organismo.

³⁶ La Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE núm. 167 de 13 julio 2022, LIITND), se aplica -entre otros ámbitos- a la IA [artículo 3.1.o) LIITND], y prevé medidas para lograr la igualdad y no discriminación cuando se utilicen mecanismos automatizados de toma de decisiones (artículo 23 LIITND).

³⁷ En la Exposición de motivos introductoria de la Instrucción CGPJ se da cuenta de los trabajos que vienen desarrollándose en este sentido, que incluyen los sistemas de IA capaces de elaborar borradores de sentencias (apartado V), si bien -como veremos- la Instrucción CGPJ se ocupa de delimitar las condiciones para el uso de estos sistemas.

³⁸ Puede verse online el Asistente de documentos con IA (del Ministerio de la presidencia, justicia y relaciones con las Cortes), para la anonimización y el resumen de documentos, aplicación dirigida especialmente a los profesionales de la justicia: [ADIA - Asistente de Documentos con IA - Servicio Público de Justicia](#) [fecha de consulta: 20.11.2025]. La anonimización de documentos es una exigencia de la normativa en materia de protección de datos y es expresamente impulsada por el legislador europeo en el considerando (69) RIA.

³⁹ En el considerando (179) RIA, relativo a la fecha de entrada en vigor del Reglamento de IA el 2 de agosto de 2026, se

Al desgranar las prácticas prohibidas en los anteriores apartados del citado artículo 5 RIA, el legislador europeo hace alusión directa a algunas relacionadas con la actividad judicial (y policial), que son las que aquí más nos interesan. En particular, se trata de las siguientes prácticas relativas a la jurisdicción penal⁴⁰, que -si bien están prohibidas como regla general-, no dejan de tener también excepciones o salvedades a las que debemos atender (artículo 5 RIA). Así:

- a) Si bien se prohíbe el uso de sistemas de IA para evaluar el riesgo de que una persona delinca a partir exclusivamente de sus datos o perfil personal, o basadas en sus rasgos y personalidad, se admite este uso cuando una valoración *se base en hechos objetivos y verificables* relacionados directamente con la acción constitutiva del delito⁴¹.
- b) Si bien se prohíbe en general el *uso de sistemas de identificación biométrica*⁴² *remota* «en tiempo real» en espacios de acceso público, este uso se admite cuando sea imprescindible para localizar o identificar al sospechoso de haber cometido determinados delitos, en la fase de investigación, enjuiciamiento o ejecución de sanción penal⁴³. En estos casos de excepción a la prohibición, o uso permitido de sistemas de identificación biométrica remota, estaremos ante sistemas de alto riesgo en la medida en que es posible que los resultados arrojen algún tipo de sesgo o discriminación, especialmente por razón de edad, etnia, raza, sexo o discapacidad⁴⁴.

15. Una vez apuntados, a grandes rasgos, los usos de la IA prohibidos en la práctica judicial, me referiré a continuación a los sistemas de IA que están admitidos, distinguiendo entre ellos muy particularmente a los considerados de alto riesgo, que tienen un régimen más estricto.

B) Los usos admitidos y la distinción de los sistemas de alto riesgo

16. En relación con el uso de la IA por parte de jueces y magistrados, es importante distinguir entre los sistemas de IA avanzada (que funcionan con cierta autonomía), y los sistemas de IA menos complejos. Como vimos, el Reglamento de IA se ocupa principalmente de los primeros, habida cuenta de que la definición de IA que toma como punto de partida se refiere a ellos en particular. Sin embargo, en la legislación nacional anterior al citado Reglamento europeo, se tienen en cuenta unos y otros indistintamente, por lo que en este apartado trataremos de dar una visión de conjunto.

indica que las prohibiciones se tendrán en consideración como riesgos inaceptables incluso con anticipación, *por ejemplo, en el ámbito del Derecho civil*.

⁴⁰ Habida cuenta de la relevancia que va a tener en el futuro el dominio de estos márgenes de actuación no siempre claramente definidos en el Reglamento de IA, por más que se haya intentado a través de una normativa detallada, la doctrina española ha publicado ya aportaciones de interés al respecto. Entre ellas, la obra colectiva titulada *La inteligencia artificial y su aplicación en el sistema de justicia penal* (2025), dirigida por M^a Lourdes Noya Ferreiro y coordinada por M^a Ángeles Catalina Benavente (Aranzadi), cuenta con interesantes aportaciones en la materia. En esta obra, por ejemplo, se defiende que el juez de lo penal no puede dictar sentencia basándose en un pronóstico elaborado por un sistema de IA, ya que éste no es apto para valorar la peligrosidad del delincuente, aspecto que incide en la *fundamentación de la agravante por reincidencia* y en la adopción de medidas tales como la *libertad vigilada* o en la *sustitución de las penas privativas de libertad* [G. QUINTERO OLIVARES, «Los límites de la aportación de la Inteligencia Artificial al derecho penal», en *La Inteligencia artificial y su aplicación en el sistema de justicia penal*, M.L. Noya (dir.)/M.A. Catalina (coord.), Aranzadi, 2025, pp. 21-46, pp. 41]. Lo anterior lleva al autor a rechazar la posibilidad de que pueda dictarse sentencia utilizando un sistema de IA en los casos en que hay que valorar la peligrosidad del delincuente, porque el sistema de IA hace valoraciones en función de experiencias ajenas al justiciable, que es *titular del derecho a un juicio justo con todas las garantías* (p. 42).

⁴¹ Artículo 5.1.d) RIA.

⁴² Se entiende por datos biométricos los *datos personales obtenidos a partir de un tratamiento técnico específico* y que se refieran a caracteres físicos o fisiológicos, o de conducta, de una persona natural, tales como la imagen facial, las huellas dactilares o la palma de las manos (artículo 3.34 RIA).

⁴³ Artículo 5.1.h) iii) RIA.

⁴⁴ Considerando (54) RIA. Se excluyen expresamente de la consideración de sistemas de IA de alto riesgo tanto los sistemas biométricos que se destinan a la autenticación de personas físicas (con el fin de confirmar que son quienes dicen ser), como los dirigidos en exclusiva a facilitar la ciberseguridad y la protección de datos. Sin embargo, se consideran de alto riesgo los destinados a conocer las emociones a partir del uso de datos biométricos.

a) Los usos admitidos en el panorama nacional

17. En el panorama nacional, la apuesta por la digitalización de la Administración de Justicia es clara, aunque -como afirma Sonia Calaza López, con su característica expresividad- *el compromiso institucional con la Justicia se asienta más en grandilocuentes palabras que en consistentes inyecciones económicas*⁴⁵.

A la espera de la aprobación y publicación de una ley para el uso y gobernanza de la IA⁴⁶, que quizás detalle algo más en este ámbito, la normativa vigente no sólo no descarta la *actuación judicial automatizada*, sino que la prevé expresamente como práctica procesal: Ya lo hizo el legislador en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (BOE núm. 160 de 6 julio 2011)⁴⁷, y ha seguido en la misma línea al derogarla con el 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^{48, 49}. A la vez, el Real Decreto-Ley 6/2023 citado, excluye expresamente el automatismo en aquellas funciones del juez que requieran interpretación jurídica, solución corroborada por la Instrucción CGPJ, como veremos a continuación.

Del Real Decreto-Ley 6/2023, cabe aquí destacar los siguientes aspectos:

- (1º) En su exposición de motivos, el legislador deja constancia de que la transformación digital de la Administración de Justicia está al servicio de los ciudadanos, y de su derecho a la tutela judicial efectiva, con el claro fin de agilizar trámites y facilitar el acceso a la Justicia, *respetando como esencia insustituible de la potestad jurisdiccional las misiones de juzgar y hacer ejecutar lo juzgado*⁵⁰.
- (2º) El artículo 56.2 dispone que los sistemas automatizados de la Administración de Justicia se utilizarán para *actuaciones de trámite o resolutorias simples, que no requieren interpretación jurídica*, entre las que se encuentran tanto la numeración o paginación de expedientes, como la *comprobación de representaciones*, o la *declaración de firmeza* cuando proceda⁵¹.
- (3º) El artículo 1.3 del Real Decreto-Ley citado, subraya el carácter *instrumental* de la tecnología, que sirve de *soporte y apoyo* a la jurisdicción, *con pleno respeto a las garantías procesales y constitucionales*; En concreto, el artículo 57 del Real Decreto-Ley 6/2023, especifica que son *actuaciones asistidas* aquellas para las que el sistema de IA genere *un borrador total o parcial de documento complejo basado en datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal*, sin que *en ningún caso* pueda considerarse ese borrador una resolución judicial ni procesal, pues para ello se requiere imperativamente la intervención humana de la auto-

⁴⁵ S. CALAZA LÓPEZ, «¿Qué pesa más en la balanza de la IA judicial, la transparencia o la protección de datos?», en *Inteligencia artificial y protección de datos. Desafíos en la era digital*, Colex, 2025, pp. 15-18, p. 16.

⁴⁶ Al respecto, puede verse el Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial (Secretaría de Estado de digitalización e inteligencia artificial, Ministerio para la transformación digital y de la función pública).

⁴⁷ El artículo 42 preveía la programación de sistemas informáticos al efecto, con el correspondiente *control de calidad*. Esta práctica la refería el legislador a actos muy variados, tales como la presentación y almacén o archivo de documentos, gestión de expedientes, tareas repetitivas (por ejemplo, la anonimización de un documento), copias, certificados, la declaración de firmeza conforme a la ley procesal, o la comunicación entre distintos sectores de la Administración.

⁴⁸ Disposición derogatoria única.

⁴⁹ El artículo 56.2 del Real Decreto-Ley 6/2023, enumera -entre otras actuaciones automatizadas- las siguientes: La numeración de los expedientes y su paginado; el envío de asuntos al archivo cuando proceda; la generación de copias, certificados y libros; la comprobación de documentos de representación; y la declaración de firmeza conforme a la ley procesal.

⁵⁰ Exposición de motivos, apartado II, párrafo 14. En el mismo apartado se explica que la norma potencia el *expediente judicial electrónico* (al menos en lo relativo al acceso a la justicia, identificación y firma de los intervinientes no presenciales), así como la interoperabilidad de los diversos sistemas (*como mínimo*, el judicial y el fiscal en cuanto a expedientes, documentos y datos se refiere).

⁵¹ Esta última robotización no se ha implementado hasta el momento (A. PERALTA GUTIÉRREZ, «Impacto comparado de la IA en la Administración de Justicia», en *La GuIA práctica de inteligencia artificial*, nº 5, noviembre 2025, Aranzadi-La Ley, pp. 1-30, p. 27).

riedad a quien corresponda (juez/a, magistrado/a, fiscal, o letrado/a de la Administración de Justicia), que es tan libre como responsable de validar o modificar el documento, de modo total o parcial.

En el mismo sentido, la Instrucción CGPJ detalla las finalidades para las que los jueces y magistrados pueden hacer uso de los sistemas de IA: En primer lugar, para buscar *información jurídica*, lo que incluye tanto la normativa como la doctrina y la jurisprudencia, así como la *recuperación de antecedentes procesales o documentales*; en segundo lugar, para analizar, clasificar y estructurar *información, documentos o datos contenidos en actuaciones judiciales*; en tercer lugar, para elaborar *esquemas, resúmenes o borradores de trabajo*, si bien estos no pueden ni tener carácter decisorio ni reemplazar la *redacción personal* de las decisiones judiciales; y, en cuarto lugar, para el desarrollo de tareas de apoyo a la preparación del trabajo jurisdiccional [artículo Sexto (*Usos permitidos de los sistemas de IA en el ejercicio de la actividad jurisdiccional*)], apartado 3, Instrucción CGPJ].

Llegados a este punto, queda clarificada la pregunta de si -conforme al Derecho nacional- puede un juez o un magistrado utilizar un sistema de IA para dictar una resolución judicial. Con todo, el CGPJ ha optado por ser aún más explícito y, en el apartado 4 del mismo artículo Sexto de la Instrucción de enero de 2026 que estamos citando, especifica que el uso de sistemas de IA para elaborar un borrador de resolución judicial sólo puede hacerse conforme a lo que dispone en el artículo Séptimo (*Borradores de resoluciones judiciales o procesales*); esto es, que los borradores de una resolución judicial estén generados por sistemas de IA facilitados por la Administración competente o por el CGPJ (que, como antes se indicó, son los únicos que pueden utilizarse para el ejercicio de la función jurisdiccional en España); que sean validados personalmente por el juez una vez revisados del todo de modo crítico; que *en ningún caso* tengan efecto automático; y que se generen sólo por voluntad del juez o magistrado, que podrá modificarlos con libertad en su totalidad. Y no se queda aquí el CGPJ, sino que insiste con tres ordinales más, el Octavo (*Usos no permitidos de los sistemas de IA en el ejercicio de la actividad jurisdiccional*)⁵², el Noveno (*Sistemas de IA no permitidos en el ejercicio de la actividad jurisdiccional*)⁵³, y el Décimo (*Sistemas de IA y protección de datos personales*), en los que -junto a nuevos matices (como el relativo a la protección de datos⁵⁴)- vuelve a recordar lo antes apuntado.

Como veremos a continuación, la solución es fiel a lo que dispone el Reglamento europeo de IA (si bien la Instrucción CGPJ añade el aludido requisito de que los sistemas de IA que se empleen por jueces y magistrados en el ejercicio de la función jurisdiccional en España sean exclusivamente los suministrados por la Administración competente o el Consejo General del Poder Judicial).

b) Los sistemas de alto riesgo conforme al Reglamento IA: La alusión a jueces y magistrados

18. Recordemos que, en el Reglamento europeo de IA, el legislador ha querido distinguir expresamente los sistemas de alto riesgo, esto es, los que supongan *un riesgo importante de causar un perjuicio a (...) la seguridad o los derechos fundamentales de las personas físicas*, así como los que puedan *influir sustancialmente en el resultado de la toma de decisiones* (artículo 6.3 RIA, *a contrario sensu*). Por tanto, pertenecerán a este grupo los sistemas de IA que faciliten el borrador de una resolución judicial. Sin embargo, los sistemas que ayuden a los jueces y magistrados en otro tipo de tareas no

⁵² Por su importancia en lo que aquí respecta, destacamos que la Instrucción CGPJ especifica en su ordinal Octavo que no pueden los jueces y magistrados delegar en la IA ni las tareas de *valoración de los hechos o de las pruebas*; ni las de interpretación del Derecho y su aplicación; ni las de elaboración de perfiles de personas, *predicción de comportamientos, evaluación de riesgos o clasificación de sujetos, fuera de los supuestos expresamente autorizados*.

⁵³ Se aclara en este ordinal Noveno de la Instrucción CGPJ que los jueces y magistrados no pueden incorporar datos judiciales a los sistemas de IA facilitados por la Administración competente o el CGPJ (únicos admitidos como ayuda en el desempeño de la actividad judicial en España), pero sí pueden utilizar estos sistemas para elaborar resúmenes, traducciones, o analizar *fuentes jurídicas, doctrinales o técnicas* si las fuentes utilizadas son de uso legítimo [párrafo segundo del ordinal Noveno, en relación con la definición de *fuentes abiertas* del ordinal Tercero, letra g), de la Instrucción CGPJ].

⁵⁴ En relación con la protección de datos personales en este ámbito, junto a lo dispuesto en el ordinal Décimo, puede verse también el ordinal Octavo, letra d), de la Instrucción CGPJ.

quedan sometidos al rigor y exigencias de los requisitos⁵⁵ que deben cumplir los sistemas de alto riesgo, pues no entran en esta catalogación (artículo 6.3 RIA).

Si bien es cierto que el legislador emplea un criterio genérico al explicar, que no entrañan *un riesgo considerable* de provocar un daño los sistemas de IA *que no influyen sustancialmente en la toma de decisiones*, entendiendo por tales aquéllos que en ningún caso afectan al *fondo, ni por consiguiente al resultado, de la toma de decisiones*, sea o no automatizada, también lo es que enumera una serie de condiciones que -de concurrir (una o varias de ellas)- justificarían que un sistema de IA pueda excluirse de los calificados como de alto riesgo⁵⁶. Estas condiciones son las siguientes:

- 1ª Que se refiera a *una tarea de procedimiento delimitada* (por ejemplo, la estructuración de datos; la clasificación de documentos; o la detección de duplicados; entre otras).
- 2ª Que se trate de una tarea consistente en la mejora de una actividad humana previa (por ejemplo, mejora del lenguaje dándole *un tono profesional* o académico, entre otros).
- 3ª Que el sistema de IA se utilice como herramienta para detectar *patrones de toma de decisiones o desviaciones* en relación con patrones previos de toma de decisiones (por ejemplo, detectando posibles incoherencias o anomalías), sin suplir la supervisión humana.
- 4ª Que la tarea esté al servicio de una evaluación humana posterior (por ejemplo, una indexación; la traducción de textos; la búsqueda; la conexión de datos; o el tratamiento de textos y *del habla*).

19. Parece claro que en la redacción del texto de una resolución judicial no concurre ninguna de las anteriores condiciones: Introducir en una aplicación informática los hechos de un caso (*input*), con la finalidad de que el sistema de IA emita el borrador de una sentencia o de un auto judicial, excede cualquiera de las tareas enumeradas y produce un resultado (*output*) capaz de influir en la toma de decisiones del juez, magistrado o, en su caso, del operador de un MASC. Por esta razón, no cabe excluir ese sistema de ser catalogado como sistema de IA de alto riesgo, consideración que lleva asociada de modo imperativo la supervisión humana, entre otros requisitos que consideraremos en el siguiente epígrafe.

Es más, la principal alusión al uso de la IA por jueces y magistrados en el Reglamento de IA aparece en su anexo III.8 RIA⁵⁷: En él se declaran sistemas de alto riesgo los *destinados a ser utilizados por una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación del Derecho a un concreto conjunto de hechos*⁵⁸. La norma se extiende a los medios alternativos de solución de conflictos (MASC), tales como la negociación, o un acto de conciliación, de mediación, o el arbitraje.

20. En el apartado 6 del mismo anexo III, se declaran de alto riesgo los sistemas de IA empleados para garantizar el cumplimiento del Derecho, con funciones tales como la elaboración de *perfiles de personas físicas* o la evaluación por la autoridad competente de la *fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos*, o bien la evaluación de *rasgos y características de la personalidad o comportamientos delictivos pasados*, usos que estarían también en principio permitidos siempre que el sistema cumpla con los requisitos exigidos para los sistemas de alto riesgo (anexo III.6 RIA)⁵⁹. Lo mismo puede decirse de los polígrafos y herramientas semejantes dirigidas a detectar si una persona dice la verdad⁶⁰.

⁵⁵ Artículos 6 y 8-15 RIA.

⁵⁶ Considerando (53) RIA.

⁵⁷ Al anexo III, titulado *Sistemas de IA alto riesgo a que se refiere el artículo 6, apartado 2*, se remite -como el título indica- el artículo 6.2 RIA, siendo el artículo 6 el dedicado a las *reglas de clasificación de los sistemas de IA de alto riesgo*.

⁵⁸ La cita textual del anexo III.8 RIA en la versión oficial en español publicada en EUR-Lex expresa este último inciso del siguiente modo: *así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos*. En la versión inglesa (a mi juicio, más clara), se dice *and in applying the law to a concrete set of facts*. Puede verse también el considerando (61) RIA.

⁵⁹ Los sistemas de IA destinados a elaborar perfiles de personas físicas se consideran siempre de alto riesgo, sin que se aplique en ningún caso lo dispuesto en el primer párrafo del artículo 6.3 RIA para evitar dicha clasificación (artículo 6.3, último párrafo, RIA).

⁶⁰ Considerando (59) RIA.

21. Estos sistemas de IA son considerados sistemas de alto riesgo en la medida en que su uso puede afectar a la dignidad humana, y a derechos tales como *el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración*, entre otros⁶¹.

Al calificarlos como sistemas de alto riesgo, el Reglamento IA admite que tanto las autoridades judiciales⁶² como los operadores de los MASC, utilicen sistemas de IA para el desempeño de sus funciones más importantes, esto es, las citadas investigación e interpretación de hechos y textos normativos⁶³, y la aplicación del Derecho a los hechos concretos objeto de la controversia⁶⁴. Lo anterior no excluye que determinados usos de sistemas de alto riesgo puedan quedar prohibidos por imperativo de otras normas, tales como la legislación en materia de protección de datos personales, que por esta razón deberán ser tenidas en cuenta⁶⁵.

22. Como necesaria contrapartida a la admisibilidad del uso de sistemas de alto riesgo, su puesta en el mercado requiere un control más exigente en cuanto a los requisitos que deben concurrir tanto para su puesta en circulación como para el control de su seguimiento y resultados, con la consiguiente responsabilidad por los posibles incumplimientos (en cuanto susceptibles de producir un daño), que pesa sobre los productores⁶⁶ y los responsables del despliegue⁶⁷ de estas herramientas tecnológicas⁶⁸. Por ejemplo, se requiere que los sistemas de alto riesgo cuenten con un sistema de gestión de riesgos establecido por el proveedor, cumplan con los adecuados estándares de calidad, o que sean aptos tanto para la conservación de registros como para la transparencia y la supervisión humana, entre otras exigencias que se detallarán a continuación.

2. Requisitos de los sistemas de IA de alto riesgo

23. La puesta en el mercado de sistemas de IA de alto riesgo no se autorizará al proveedor, a menos que se garanticen las medidas necesarias para proteger la salud, la seguridad, y los derechos fundamentales de las personas⁶⁹. Junto a otros requisitos (tales como la calidad y el sistema de gestión

⁶¹ Considerando (48) RIA. Para clasificar un sistema como de alto riesgo se tiene en cuenta tanto la gravedad del daño que puede producir, como su probabilidad [considerando (52)].

⁶² Según explica M. BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*], Francis Lefebvre, 2025, p. 108, 750], por *autoridad judicial* debe comprenderse tanto fiscales y funcionarios judiciales, como jueces y magistrados.

⁶³ Como también ha explicado M. BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*], Francis Lefebvre, 2025, p. 108, 750], la referencia a la ley incluye a los reglamentos y cualquier norma jurídica.

⁶⁴ Conforme indica M. BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*], Francis Lefebvre, 2025, pp. 108-109, 752] se admiten aquí no sólo los *sistemas de asistencia que estructuran y resumen expedientes*, o los que *sugieren fuentes que deben tenerse en cuenta* (por ejemplo, *resoluciones judiciales o bibliografía académica*), sino también los que *preparan borradores de resolución*.

⁶⁵ El legislador tiene interés en dejar constancia de ello. Puede verse en este sentido el considerando (63) RIA.

⁶⁶ A efectos de garantizar la seguridad jurídica, en determinadas circunstancias relacionadas con sistemas de alto riesgo (por ejemplo, cuando se ponga en él un nombre o marca comercial, o si modifica el sistema de alto riesgo), se considera proveedor a *cualquier distribuidor, importador, responsable del despliegue u otro tercero*, que asumirá las obligaciones correspondientes [considerando (84) RIA].

⁶⁷ Los responsables del despliegue deben evaluar su impacto en los derechos fundamentales antes de la puesta en funcionamiento (y actualizar la evaluación, si cambian los factores de impacto), a fin de determinar los riesgos que existen para las personas que puedan resultar afectadas y definir las *medidas que deben adoptarse* en caso de materializarse alguno de esos riesgos [Considerando (96) RIA]. El legislador se refiere, en concreto, a los responsables del despliegue cuando sean, bien *organismos de Derecho público*, bien *entidades privadas que presten servicios públicos*, o bien *entidades bancarias o de seguros*.

⁶⁸ Considerandos (79) y (84) RIA.

⁶⁹ Como ha explicado M. BARRIO ANDRÉS [*Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*], Francis Lefebvre, 2025, p. 78, 501), *los sistemas de IA que el legislador de la Unión considera que plantean un riesgo elevado, pero no inaceptable, están sujetos a obligaciones muy estrictas a fin de preservar los valores y derechos fundamentales de la UE*.

de riesgos)⁷⁰, hay tres mecanismos de defensa o principios rectores en materia de sistemas de IA de alto riesgo que presentan especial interés desde la perspectiva que aquí estamos tratando. Son los siguientes: (1º) que el sistema de IA esté habilitado para la supervisión humana; (2º) que esté habilitado para la transparencia; y, (3º) que esté habilitado para la trazabilidad. Veamos qué repercusión tienen estos requisitos en relación con el trabajo de jueces y magistrados que utilicen sistemas de IA avanzada como apoyo en el desempeño de sus funciones.

A) La supervisión humana

24. La supervisión humana viene exigida en el artículo 14 del Reglamento IA, con el objetivo de proteger a la persona humana y, en particular, su salud, seguridad y derechos fundamentales (artículo 14.2 RIA). La persona no se confía en absoluto al mero cuidado de una máquina, por muy perfecta que sea. Por el contrario, se pretende *prevenir o reducir al mínimo* el riesgo que corren sus derechos fundamentales, en concreto si estos riesgos persisten a pesar del cumplimiento de los restantes requisitos exigidos a los sistemas de IA de alto riesgo.

Con este fin, se dispone que los sistemas sean supervisados o *vigilados de manera efectiva por personas físicas* mientras se hace uso de ellos, tarea que implica el uso de las herramientas adecuadas, garantizado por el proveedor⁷¹. En la práctica judicial, el requisito de la supervisión humana evita que un auto o sentencia sea expedido de modo automático con eficacia frente a terceros, sin validación previa de la autoridad competente, juez o magistrado.

25. El Reglamento de IA precisa que al menos un profesional evalúe los resultados arrojados por el sistema de IA consultado, con la responsabilidad de contrastarlos debidamente y -según el caso- corregirlos o confirmarlos. Aunque el artículo 14 RIA, relativo a la supervisión humana, es genérico y no está dedicado al ejercicio de una concreta profesión, sí hace alusión particular, en su último apartado, al uso de sistemas de IA de alto riesgo *con fines de garantía del cumplimiento del Derecho*, para admitir que la verificación pueda realizarse por una sola persona física.

Una excepción a lo anterior la constituyen aquellos casos en que, para la obtención de resultados, se hubiera trabajado con un sistema de identificación biométrica remota, pues el Reglamento de IA

⁷⁰ Junto a los requisitos de transparencia, trazabilidad y supervisión humana, los sistemas de IA de alto riesgo deben cumplir también los siguientes requisitos:

(1) Se debe establecer y mantener un sistema de gestión de riesgos que revise en primer lugar los riesgos para la salud, seguridad y derechos fundamentales [artículo 9.2.a) RIA]. Al respecto, pueden verse los considerandos (64) y (65).

(2) Debe garantizarse la calidad de los datos suministrados a los sistemas de IA de alto riesgo, y con esta finalidad *se someterán a prácticas de gobernanza y gestión de datos* centradas, entre otros aspectos, en examinar si existen sesgos que puedan afectar negativamente a la salud, seguridad y derechos fundamentales de las personas [artículo 10.2.f) RIA], y se procurará que los datos suministrados al sistema carezcan de errores y sean lo más completos posible con vistas a su finalidad (artículo 10.3 RIA). Son responsables del sistema de gestión de la calidad los proveedores (artículo 17 RIA), que deberán también conservar la documentación correspondiente [artículo 18.1.b) RIA].

(3) El sistema de IA de alto riesgo debe contar con la correspondiente documentación técnica antes de su puesta en el mercado, que se actualizará mientras esté en uso el sistema (artículo 11 RIA).

(4) El sistema de IA de alto riesgo debe garantizar la precisión, solidez y ciberseguridad adecuada. Por ejemplo, mediante copias de seguridad o la previsión de medidas de actuación ante la aparición de posibles fallos (tales como bucles de retroalimentación), conforme al artículo 15 RIA.

Los requisitos de los sistemas de IA de alto riesgo están previstos en la Sección 2 del Capítulo III RIA (artículos 8 a 15) y a ellos se refiere el legislador en el considerando (66) y siguientes, además de en los ya citados (64) y (65) en lo que se refiere al sistema de gestión de riesgos. El cumplimiento de estos requisitos será supervisado por la autoridad de vigilancia del mercado competente, en su condición de «productos que presentan un riesgo» que afecta a la seguridad y derechos fundamentales de las personas (artículo 79 RIA).

⁷¹ El artículo 14.1 RIA se refiere en particular a herramientas de interfaz humano-máquina, es decir, a herramientas HMI (*human machine interface*), que son paneles de control que conectan al usuario con la máquina para controlar su actividad en tiempo real. Además, el legislador europeo insiste en que cuando proceda (y aquí debemos incluir los usos de estas herramientas por jueces y magistrados), el sistema garantice que *las personas físicas a quienes se haya encomendado la supervisión humana* sean las competentes y autorizadas para el desarrollo de la función correspondiente [considerando (73) RIA].

requiere entonces un mínimo de dos supervisores. Aunque el legislador europeo deja expresamente en manos del legislador nacional o de la Unión decidir en qué casos sería desproporcionado el requisito de la verificación por pares, sí la exige sin embargo para la toma de decisiones basada en resultados arrojados por sistemas de identificación biométrica remota (artículo 14.5 RIA, apartados 2 y 1, respectivamente). En el considerando (73) RIA se explica la supervisión humana *reforzada* que se requiere para estos últimos⁷².

26. Para cumplir bien su cometido, el juez o magistrado debe ser consciente no sólo de las capacidades, sino de las limitaciones del sistema y de la tendencia a confiar excesivamente en ellos (lo que el Reglamento de IA denomina *sesgo de automatización*), debiendo descartar o invalidar los resultados cuando sea oportuno y bajo su personal responsabilidad (artículo 14.4 RIA). Al servicio de este conocimiento están previstas medidas de alfabetización (artículo 4 RIA) y transparencia (artículo 13 RIA).

B) La transparencia

27. Transparencia significa información, dirigida tanto al profesional usuario del sistema de IA como al tercero que pueda resultar afectado por el uso del mismo: Aunque inicialmente puede parecer que el requisito de transparencia va dirigido exclusivamente a capacitar a los responsables del despliegue para que hagan un uso e interpretación responsable del *output* o resultado proporcionado por el sistema de IA de alto riesgo (artículo 13.1 RIA), en realidad el requisito de transparencia llega más lejos.

De la lectura del Reglamento IA se desprende que el requisito de transparencia vela por la información, y lo hace en un doble sentido: De un lado, el proveedor del sistema de IA de alto riesgo debe garantizar la información del profesional usuario (o responsable del despliegue) a través de las instrucciones de uso del sistema, y de otra parte, el responsable del despliegue debe informar al tercero que pueda resultar afectado por el resultado, que se ha hecho uso de un sistema de IA de alto riesgo. Veámoslo con más detalle:

En primer lugar, la información que el proveedor debe proporcionar al responsable del despliegue o profesional usuario del sistema de IA de alto riesgo se refiere tanto a las *características, capacidades y limitaciones* del sistema, como a las medidas de supervisión humana exigidas por el Reglamento IA (incluyendo las pautas técnicas que facilitan la interpretación de los resultados *-output-* por los responsables del despliegue), entre otros aspectos (artículos 13 y 50⁷³ RIA).

En segundo lugar, el responsable del despliegue debe informar al tercero afectado sobre el uso de un sistema de IA de alto riesgo en el proceso de toma de decisiones o producción de un resultado que le concierne⁷⁴. Si analizamos esta obligación de información desde la perspectiva de la Administración de Justicia, cabe destacar los siguientes aspectos:

- 1º Desde el punto de vista del sujeto obligado, la obligación compete en particular a los jueces y magistrados, en cuanto responsables del despliegue: El artículo 26.11 del Reglamento de IA se refiere en concreto a los sistemas de IA del anexo III, entre los que recordemos se cuentan los sistemas que ayudan a tomar decisiones a jueces y magistrados (anexo III.8 RIA).
- 2º En el lado pasivo de la obligación de información se encuentran los posibles afectados. Aunque la versión inglesa del artículo 26.11 del Reglamento de IA se refiere sólo a las personas físicas o naturales (*natural persons*), entiendo que la misma regla se aplicará cuando

⁷² Además, en el considerando (159) RIA, el legislador europeo explica que las autoridades de vigilancia del mercado deben tener facultades efectivas, en relación con estos sistemas, tanto para la investigación y acceso a los datos personales tratados, como para la corrección de errores detectados (el considerando citado se refiere a facultades correctoras, sin más).

⁷³ El artículo 50.1 RIA exige que el proveedor garantice que las personas físicas que interactúen con los sistemas de IA estén informadas de ello, salvo que sea evidente.

⁷⁴ C. MUÑOZ GARCÍA, «Enfoque holístico del RIA y necesaria cohesión con otras normas a actualizar, entre otras, responsabilidad civil y Derecho de consumo», en *La evolución de los derechos subjetivos. Nuevos derechos, nuevas cuestiones jurídicas*, J. Agudo/C. Jerez (codirs.), AFDUAM (UAM-BOE), núm. 29, 2025, pp. 315-351, pp. 337-339.

el tercero sea una entidad o persona jurídica, en la medida en que esté integrada por personas físicas o éstas resulten o puedan resultar afectadas.

- 3º En cuanto al contenido de la información, será el correspondiente al uso que se ha hecho de la IA para tomar la decisión final o como ayuda para tomarla [considerandos (27) y (93) RIA, y artículo 26.11 RIA]⁷⁵.
- 4º Junto a lo anterior, cabe destacar que el Reglamento de IA crea a favor de los afectados por las decisiones basadas en la IA, un nuevo *derecho a explicación de decisiones tomadas individualmente* (artículo 86 RIA), sobre el que volveré en el apartado relativo a la responsabilidad por el abuso de sistemas de IA de alto riesgo.

28. Por lo demás, cuando los sistemas de IA no sean de alto riesgo no queda especificada esta obligación de transparencia, salvo que supongan riesgos de suplantación de la persona o engaño, en cuyo caso se aplican medidas especiales de transparencia, sean o no sistemas de alto riesgo: En este sentido, se impone la obligación de *notificar* a las personas físicas expuestas, que sus datos biométricos están siendo tratados por un sistema capaz de inferir de ellos *sus emociones o intenciones o incluirlas en categorías específicas*⁷⁶.

C) La trazabilidad

29. El requisito de trazabilidad está conectado con el de transparencia (considerando 27 RIA), y se refiere, en particular, a la conservación automática de registros (*archivo de registros*) de la actividad desarrollada con sistemas de IA de alto riesgo (artículo 12 RIA). Los *sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de acontecimientos, mediante archivos de registro, durante toda la vida útil del sistema*⁷⁷. En particular, el requisito de trazabilidad supone la obligación de que los registros tengan capacidad de almacenar los datos necesarios para detectar la situación que ha dado lugar a un daño a la salud, la seguridad o los derechos fundamentales de las personas⁷⁸, así como para facilitar la vigilancia poscomercial de los sistemas de IA de alto riesgo⁷⁹.

30. Esta exigencia permite garantizar que el uso de la IA pueda ser revisado por los responsables del despliegue (en nuestro caso, jueces y magistrados), a efectos de localizar un error por parte del sistema. En la medida en que dicho fallo pueda afectar a la seguridad o los derechos fundamentales de las personas, nace para el responsable del despliegue no sólo la consiguiente obligación de reportarlo inmediatamente al *proveedor o distribuidor y a la autoridad de vigilancia del mercado*⁸⁰ pertinente,

⁷⁵ En particular, el legislador europeo explica el papel que desempeñan los responsables del despliegue en la información a los afectados, cuando utilicen sistemas de alto riesgo cuyos resultados afecten a la toma de decisiones relacionadas con ellos [considerando (93) RIA].

⁷⁶ Considerando (132) RIA.

⁷⁷ Considerando (71) RIA.

⁷⁸ Así se deduce de lo dispuesto en el artículo 12.2 RIA, en conexión con los artículos citados en él (en particular el artículo 79.1 RIA, al que también alude el artículo 26.5 RIA). El artículo 20.2 RIA dispone que tanto el proveedor como el responsable del sistema investiguen las causas de los riesgos de que un sistema afecte negativamente a la salud, seguridad o derechos fundamentales de las personas, y lo comuniquen a la correspondiente autoridad de vigilancia del mercado. El importador, por su parte, está obligado a informar al proveedor y, en su caso, al representante autorizado en la UE del proveedor, así como a las autoridades de vigilancia del mercado, si el sistema de IA de alto riesgo puede afectar negativamente a la salud, seguridad o derechos fundamentales de las personas (artículo 23.2 RIA). Idéntica obligación corresponde al distribuidor de un sistema de IA de alto riesgo, que debe comunicarlo al proveedor o -en su caso- importador del producto (artículo 24.2 y 24.4 RIA).

⁷⁹ Conforme a las medidas previstas en el artículo 72 RIA.

⁸⁰ En los ámbitos que aquí estamos tratando, las autoridades previstas para garantizar la conformidad de las mercaderías [conforme a lo dispuesto en el Reglamento (UE) 2019/1020, del Parlamento europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos] pudieran ser, si se aprueba el Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial (Ministerio para la transformación digital y de la función pública, Secretaría de Estado de digitalización e inteligencia artificial, 2025), las siguientes: De un lado, la Dirección de supervisión y control de protección de datos del Consejo General del Poder Judicial, para los sistemas de IA de alto riesgo utilizados por la Administración de Justicia conforme a lo previsto en el Anexo III.8.a) RIA, y de otro lado, la Agencia Española de Protección

sino la de suspender el uso del sistema. Si el incidente es grave, se notificará a todos ellos (artículo 26.5 RIA).

Lógicamente, el archivo de registros permitirá además detectar un uso indebido del sistema que haya podido causar un daño a tercero, aspecto importante a efectos de exigir responsabilidad al causante del daño. Por esta razón, debemos prestar atención a factores tales como quién o quiénes son los sujetos obligados a conservar los archivos, y durante cuánto tiempo están obligados a conservarlos.

31. La obligación de conservar los archivos corresponde tanto al proveedor del sistema de IA de alto riesgo (en la medida en que *estén bajo su control*), como a los responsables del despliegue (también en la medida en que *estén bajo su control*), siendo -en ambos casos- el tiempo mínimo de conservación de los archivos, de seis meses (artículos 19.1 y 26.6 RIA, respectivamente). Sin embargo, puesto que la trazabilidad está al servicio de la finalidad a la que se destina el sistema de IA de alto riesgo (artículo 12.2 RIA), es posible afirmar que ese plazo de conservación de archivos será superior a seis meses cuando la finalidad del sistema sea facilitar el trabajo de la Administración de Justicia. En estos casos, a mi juicio, deberá conservarse la documentación mientras los resultados puedan afectar a terceros. Aunque el legislador europeo deja abierta la posible regulación de la materia del plazo de conservación de estos archivos de registros, sea por el legislador de la Unión, sea por el nacional, sí se ocupa de indicar que deben conservarse por quien tenga el sistema bajo control -sea el proveedor, sea el responsable del despliegue- *durante un periodo de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo* (artículos 19.1 y 26.6 RIA, respectivamente).

3. La responsabilidad por el abuso de los sistemas de IA de alto riesgo.

32. Siguiendo la terminología del Reglamento IA, son responsables del despliegue las personas físicas o jurídicas, autoridades públicas, órganos u organismos que utilicen con fines profesionales un sistema de IA *bajo su propia autoridad* [artículo 3.4) RIA]. La expresión «bajo su propia autoridad» *debe entenderse como la asunción de responsabilidad sobre la decisión de desplegar el sistema y sobre la forma de su uso real en la práctica*⁸¹. Por tanto, los responsables del despliegue son sujetos activos de la responsabilidad por el uso que hagan de los sistemas de IA de alto riesgo bajo su autoridad, cuando se cause daño a terceros.

El uso de la IA se convierte en mal uso o abuso cuando se infringe la obligación de velar por la salud, seguridad y los derechos fundamentales de la persona, la democracia, el Estado de Derecho, o el medio ambiente, que sería contrario a los objetivos del Reglamento de IA (artículo 1 RIA). Entre otras, corresponde entonces aplicar las medidas de responsabilidad civil dirigidas a reestablecer al perjudicado en la situación en que estaría en el caso de que se hubiera actuado diligentemente, esto es, en caso de haberse hecho buen uso de la IA. Es de aplicación aquí, entretanto no exista una norma especial al efecto⁸², lo dispuesto en el Derecho común: En concreto el sistema de responsabilidad civil, contractual -cuando proceda- y extracontractual (conforme al cual, quien causa daño a otro interviniendo culpa o negligencia -sea por acción, sea por omisión- está obligado a indemnizar el daño causado)⁸³.

de Datos y las autoridades autonómicas de protección de datos para lo que se refiere a sistemas de IA de alto riesgo empleados para garantizar el cumplimiento del Derecho conforme a lo previsto en el Anexo III.6 RIA.

⁸¹ M. BARRIO ANDRÉS, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, p. 26, 97.

⁸² Al parecer, no llegará a aprobarse la proyectada directiva sobre responsabilidad en materia de IA, esto es, la Propuesta de Directiva del Parlamento europeo y del Consejo, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Bruselas, 28.9.2022). En España, la responsabilidad civil extracontractual está regulada por el Derecho común (artículos 1902 y siguientes CC), complementado -ocasionalmente- por leyes especiales (tal es el caso de la responsabilidad de los jueces y magistrados, como veremos a continuación).

⁸³ Si estuviéramos hablando del trabajo de los operadores jurídicos de los MASC, pudiéramos hablar de responsabilidad contractual en la medida en que su trabajo se haya concertado mediante un contrato, directamente o a través de una entidad, por ejemplo, de mediación, conciliación y/o arbitraje. En el caso de los jueces y magistrados, la responsabilidad de la Administración de Justicia frente al tercero afectado será de naturaleza extracontractual. Como concluye Carmen MUÑOZ GARCÍA

A nivel nacional, la Agencia Española de Supervisión de la IA (AESIA, dependiente de la Secretaría de Estado de Digitalización e IA del Ministerio para la Transformación Digital y de la Función Pública), se ha creado con la finalidad, entre otras, de supervisar *la puesta en marcha, uso o comercialización* de sistemas que incluyan IA, en particular aquéllos que mayor riesgo supongan para la salud, seguridad y derechos fundamentales de las personas. En relación con el sector de la Justicia, se delegan competencias en el Consejo General del Poder Judicial⁸⁴.

33. Si atendemos en particular a la responsabilidad de jueces y magistrados -penal, civil y/o disciplinaria⁸⁵-, podemos preguntarnos qué uso de los sistemas de IA de alto riesgo por estos profesionales en el desempeño de sus funciones puede causar un daño a tercero del que deban responder, o bien, cuándo podemos hablar de un mal uso o abuso de los sistemas de IA de alto riesgo.

El daño derivado del uso de un sistema de IA de alto riesgo por el juez o por el magistrado, puede tener lugar por una acción o por una omisión en el desempeño de la función jurisdiccional. Si tenemos en cuenta que un sistema de IA capaz de preparar un borrador de una resolución judicial o sentencia tras la introducción de los hechos del caso es un sistema de IA de alto riesgo y, por tanto, su uso sólo está permitido en la medida en que exista supervisión humana, todos coincidiremos en afirmar que el requisito de supervisión no se cumple de modo exclusivamente formal, sino que debe existir en todo caso una acción positiva, real y eficaz, de supervisión: Supervisar implica *prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales* (artículo 14.2 RIA). La máquina no debe realizar el trabajo del juez o magistrado, aunque pueda agilizarlo o facilitarlo. En este sentido, la Instrucción CGPJ no admite que los jueces y magistrados incorporen a resoluciones judiciales textos generados por la IA sin que exista antes *una validación crítica, completa y personal* por su parte⁸⁶.

Por esta razón, la responsabilidad del juez o magistrado (o primeramente del Estado, si nos referimos al ámbito civil) por un mal uso o abuso de la IA, comienza con el incumplimiento del deber de supervisión de los resultados arrojados por el sistema de IA de alto riesgo consultado. Debemos distinguir entre la supervisión formal o formalizada, y la supervisión real y eficaz. El hecho de que estos sistemas lleven incorporado por exigencia del Reglamento IA un dispositivo para garantizar que el resultado de una consulta no pueda ser directamente ejecutable frente a los particulares afectados, sino que requiera intervención humana, no garantiza en absoluto que la supervisión real y eficaz haya tenido lugar, sino que sencillamente facilita localizar a la persona responsable del daño, en caso de producirse.

34. La omisión de la supervisión humana, real y eficaz, significa un mal uso o abuso de la IA en el contexto que estamos tratando. Constituye imprudencia grave que el juez o magistrado se apoye en los resultados de la búsqueda sin una supervisión real y eficaz, hecho que dará lugar a responsabilidad si como consecuencia se dicta una resolución injusta provocando un daño. Si se dicta una resolución injusta en ausencia de supervisión real y se provoca con ello un daño a tercero, el hecho de haber clicado la casilla correspondiente a la supervisión de los resultados (supervisión formal) no obsta a que nazca la responsabilidad correspondiente; y lo mismo cabe decir de una supervisión realizada con negligencia grave por parte del juez o magistrado, que haría ineficaz el acto mismo de supervisión. En ambos casos

[«Enfoque holístico del RIA y necesaria cohesión con otras normas a actualizar, entre otras, responsabilidad civil y Derecho de consumo», en *La evolución de los derechos subjetivos. Nuevos derechos, nuevas cuestiones jurídicas*, J. Agudo/C. Jerez (codirs.), AFDUAM (UAM-BOE), núm. 29, 2025, pp. 315-351, p. 348], en relación con los posibles daños derivados del uso de la IA, *siempre nos quedará la responsabilidad civil, contractual y extracontractual*.

⁸⁴ M. BARRIO ANDRÉS, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, pp. 237-238, 2345, 2347 y 2348. El autor hace alusión a la normativa autonómica valenciana, extremeña y gallega, en materia de IA (p. 239, 2350). Al respecto, véanse los considerandos I (párrafo tercero) y III-V de la Instrucción CGPJ, así como su ordinal Quinto (*Sistemas de IA permitidos en el ejercicio de la actividad jurisdiccional*, segundo párrafo); y, en relación con la protección de datos, su ordinal Duodécimo (*Supervisión y control del Consejo General del Poder Judicial*).

⁸⁵ No abordaré aquí la responsabilidad disciplinaria. Al respecto, puede verse: B. ANGLÈS JUANPERE, «La responsabilidad de jueces y magistrados», *Revista CEFLEGAL*, n.º 134, 2012, pp. 107-142. El autor aborda la responsabilidad penal, civil (aunque en este punto hay que tener en cuenta la supresión posterior de los artículos correspondientes en la LOPJ, por la reforma de 2015), y disciplinaria de los jueces y magistrados.

⁸⁶ Ordinal Octavo, letra c), Instrucción CGPJ.

concurren todas las circunstancias jurídicamente relevantes para que la víctima pueda exigir una indemnización o compensación del daño por responsabilidad civil extracontractual, esto es, concurren la omisión o la acción culpable, el daño, y el nexo causal entre lo primero y lo segundo (artículo 1902 CC)⁸⁷.

35. Desde la perspectiva penal, hay que contemplar la posibilidad de incurrir en delito de prevaricación por un mal uso por el juez o magistrado de un sistema de IA de alto riesgo (artículo 447 CP), mientras que la perspectiva civil nos conduce a la posible responsabilidad patrimonial del Estado, propia de la actuación de jueces y magistrados.

36. En España, así como la responsabilidad penal de los jueces y magistrados se rige por el Código penal (CP), su responsabilidad civil se redirige -como veremos- a las normas de la responsabilidad patrimonial del Estado, aunque -cuando se trate de responsabilidad civil derivada de delito- pudiera solicitarse por la vía penal [artículo 37 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (BOE núm. 236 de 2 octubre 2015), LRJSP, y artículo 115 CP]⁸⁸. Si bien es cierto que el Estado debe responder frente a la víctima del daño con el pago de la indemnización correspondiente, también lo es que podrá después repetir el cobro frente al juez o magistrado que actuó con culpa grave⁸⁹ o con dolo, sin perjuicio de la posible responsabilidad disciplinaria en que pudiera incurrir [artículos 106.1, 117 y 121 CE; artículos 16 y 296.2 Ley Orgánica 6/1985, de 1 de julio, del Poder judicial (BOE núm. 157 de 2 julio 1985), LOPJ; artículo 36 LRJSP; y, subsidiariamente, artículo 1902 CC]⁹⁰. La Instrucción CGPJ deja claro que el juez o magistrado que recurra al uso de un sistema de IA lo hará bajo su *exclusiva responsabilidad*⁹¹.

Desde la Ley 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder judicial (BOE núm. 174 de 22 julio 2015), el perjudicado carece de acción directa frente al juez o al magistrado para reclamar la indemnización por responsabilidad civil y debe solicitarla vía responsabilidad patrimonial por error judicial o por funcionamiento anormal de la Administración de Justicia, lo que implica la necesidad de obtener previa resolución judicial de reconocimiento del error, que a su vez debe instarse en un plazo de tres meses (artículos 292 y siguientes LOPJ). Para exigir la responsabilidad civil correspondiente, de naturaleza extracontractual, se aplican primeramente las reglas de la responsabilidad patrimonial del Estado⁹², es decir, la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE núm. 174 de 22 julio 2015, LPACAP, artículos 91 y 92), y los artículos 32 a 35 LRJSP. Si, presentada la acción, no se resuelve en el plazo de

⁸⁷ Desde una perspectiva de Derecho internacional privado europeo, A. ORTEGA GIMÉNEZ («Competencia judicial internacional y necesaria cohabitación entre el Reglamento “Bruselas I bis”, el Reglamento General de Protección de Datos de la UE y el nuevo Reglamento europeo de Inteligencia Artificial», *Revista española de Derecho internacional*, vol. 77, 2025, 2, pp. 237-255) ha puesto de relieve las dificultades para determinar la competencia judicial internacional cuando proceda, si -como consecuencia de un mal uso de la IA- se ha causado un daño resarcible por responsabilidad civil extracontractual.

⁸⁸ En su apartado segundo, este artículo especifica que *la exigencia de responsabilidad penal del personal al servicio de las Administraciones Públicas no suspenderá los procedimientos de reconocimiento de responsabilidad patrimonial* iniciados, salvo que sea necesario determinar los hechos en el orden penal para determinar la responsabilidad patrimonial.

⁸⁹ Se ha explicado que la responsabilidad de los jueces se aleja de la responsabilidad objetiva y se vincula por regla general a la culpa grave: *Se exige al juez que aplique todos sus conocimientos técnicos y jurídicos y la necesaria dedicación a la correcta resolución del caso* (E. ARIAS-SALGADO ROBSY, *La responsabilidad personal del juez*, Discurso de ingreso en la Real Academia de Jurisprudencia y Legislación, RAJL, Granada, 29.20.2013, p. 18, adviértase que el texto es anterior a la reforma de la LOPJ de 2015, que suprimió la responsabilidad civil directa de los jueces y magistrados, sin que la reforma afecte a lo que aquí citamos). La autora añade que se incurre en responsabilidad no tanto por un desacierto como por el incumplimiento *patente* y clamoroso de la obligación citada, *causando un daño*.

⁹⁰ Según B. ANGLÈS JUANPERE («La responsabilidad de jueces y magistrados», *Revista CEFLEGAL*, n° 134, 2012, pp. 107-142, pp. 138-139), en la práctica es difícil que el Tribunal Supremo reconozca la responsabilidad del juez o magistrado, pues exige que exista una prueba incontestable de la ignorancia inexcusable o de la voluntad negligente, mientras que si se trató de un simple error o de una anomalía en el funcionamiento de la Administración judicial, será el Estado y no el juez o el magistrado quien asuma la responsabilidad. El autor se hace eco de relevante doctrina que considera insuficiente el sistema.

⁹¹ Ordinal Séptimo, apartado 2, Instrucción CGPJ. En el ordinal Undécimo (*Incumplimiento de los criterios, pautas de uso y principios*) Instrucción CGPJ, se recuerda que -en relación con la responsabilidad de los jueces y magistrados- será de aplicación lo dispuesto en la LOPJ, sin perjuicio de otras *medidas preventivas o correctoras que puedan adoptarse* por el Poder Judicial.

⁹² Salvo en la vía penal, como quedó explicado.

seis meses, se entenderá desestimada (artículo 91.3 LPACAP). La resolución debe pronunciarse sobre *la existencia o no de la relación de causalidad entre el funcionamiento del servicio público y la lesión producida y, en su caso, sobre la valoración del daño causado* (artículo 91.2 LPACAP), que ha de ser evaluable económicamente (artículo 32.2 LRJSP).

37. Corresponde al afectado probar la relación causal entre la acción u omisión del juez o magistrado (relacionada aquí con el mal uso o abuso de un sistema de IA de alto riesgo) y el daño provocado. En este punto, es interesante considerar que el legislador europeo *tuvo en cuenta la crítica fundamental al proyecto de la Comisión de que no contenía ningún derecho subjetivo para los afectados por (...) las decisiones basadas en la IA*, lo que alejaba el texto de la prometida IA centrada en el ser humano y sus derechos fundamentales, y asumió la enmienda⁹³: De este modo se consiguió no sólo que los terceros tuvieran derecho a ser informados por el uso que se hizo de un sistema de IA de alto riesgo en el proceso de toma de decisiones (como parte del requisito de transparencia), sino que además toda persona afectada negativamente por el uso de un sistema de IA de alto riesgo tenga derecho a recibir una explicación detallada -o *explicaciones claras y significativas*, según el tenor literal del Reglamento IA- por parte del responsable del despliegue, *acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada* (artículo 86.I RIA). A hacer efectivo este derecho contribuirá el registro que -conforme al principio de trazabilidad- deben contener los sistemas de IA de alto riesgo, cuyo control queda bajo responsabilidad sea del proveedor, sea del responsable del despliegue, cuando estén bajo su esfera de control⁹⁴.

Dado que la obligación de un juez o magistrado es una obligación de medios y no de resultado, a efectos de prueba, conviene añadir que la adecuada supervisión humana requiere la diligencia del profesional, y no sólo en cuanto al análisis de los resultados sino también en relación con los presupuestos de su actuación. Tratándose de un juez o un magistrado que utilice un sistema de IA para obtener un borrador de resolución o sentencia, deberán darse cuanto menos dos condiciones: Que el juez o magistrado realice adecuadamente la consulta, mediante la introducción correcta de los datos del caso (*input*) y la formulación adecuada de las cuestiones objeto de búsqueda (entre otras posibles acciones que se dan como presupuesto de la supervisión humana), y que el juez o magistrado supervise con diligencia los resultados emitidos por el sistema (el *output*), seleccionando aquéllos que sean válidos y descartando los que sean erróneos, equívocos, discriminatorios, o -en general- incorrectos. De lo contrario, la seguridad y los derechos fundamentales de la persona estarían en riesgo, pudiendo ocasionarse un incidente grave. De ahí que el uso de la IA por parte de jueces y magistrados reclame que se les facilite una seria y responsable formación previa, que debe reforzarse en tantos niveles como sea preciso, y debería requerir -a mi juicio- la consiguiente acreditación. Para evitar un mal uso o abuso de la IA, es preciso intensificar la formación que haga posible el buen uso de la IA por jueces y magistrados⁹⁵.

38. A mi juicio, junto a supuestos de responsabilidad subjetiva como los antes referidos, pueden darse también supuestos de responsabilidad objetiva. Estaríamos ante un supuesto de responsabilidad objetiva cuando el resultado de la búsqueda sea erróneo en perjuicio del afectado y no conste que el juez o magistrado haya introducido ningún cambio, pudiendo decirse que, o se limitó a validar el texto de la resolución o sentencia, como hubiera podido hacerse de modo automático por una máquina, o erró en el desempeño de su función de supervisión al no detectar errores susceptibles de causar un daño a tercero. Por muy perfecto que sea un sistema de IA de alto riesgo, el resultado erróneo de una búsqueda no ha de ser -en sí- causa de exoneración de responsabilidad del juez o magistrado (o del Estado, en su lugar), cuando se produzca un daño, sino más bien al contrario. El juez o magistrado que confía excesivamente en los resultados de la consulta omite la debida diligencia en el desempeño de sus funciones, y no podrá

⁹³ M. BARRIO ANDRÉS, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, p. 27, 100.

⁹⁴ Artículos 19.1 y 26.6 RIA. En relación con el tiempo de conservación de los registros, me remito a lo ya explicado en el apartado relativo a la trazabilidad.

⁹⁵ En España, el Consejo General del Poder Judicial se compromete a ofrecer a jueces y magistrados la debida formación (ordinal Decimotercero de la citada Instrucción CGPJ).

alegar fuerza mayor⁹⁶ -ni el Estado, en su lugar, para denegar la indemnización-, pues el daño pudo evitarse⁹⁷ si se hubiera cumplido el deber de intervenir activamente en la revisión del borrador de resolución facilitado mecánicamente.

Más aún: Una reciente sentencia argentina ha equiparado la infracción del deber de transparencia con la infracción del deber de supervisión. Se trata de un caso en el que el abogado descubrió que el juez había dictado sentencia haciendo uso de la IA, pero sin informar sobre ello, siendo el detonante del hallazgo una frase intercalada en el texto que claramente delataba dicho uso. Recurrida la sentencia, fue anulada, al declararse que *la falta de indicación sobre el modo en que se usó la inteligencia artificial en un punto decisivo, entraña un riesgo de que dicha tecnología se hubiese utilizado delegando una actividad jurisdiccional indebidamente*, y con ello se violaría el derecho a ser juzgado por una persona habilitada por el Estado para llevar a cabo esa función⁹⁸ (en España, artículo 24.2 CE).

39. Se considera un incidente grave, a efectos del Reglamento IA, el que tenga como consecuencia el incumplimiento de alguna obligación impuesta por el Derecho de la Unión para proteger los derechos fundamentales [artículo 3.49) RIA]. En el caso que estamos considerando, una de estas obligaciones es la que corresponde al juez o al magistrado de supervisar con diligencia los resultados obtenidos por un sistema de IA, pues en otro caso el uso del sistema no estaría al servicio de la persona (artículo 1 RIA, y principio de *acción y supervisión humanas*⁹⁹), sino de otros factores secundarios en relación con la finalidad principal (tales como, por ejemplo, agilizar la carga de los tribunales), y daría lugar a la consiguiente responsabilidad en caso de provocar daños.

Esta responsabilidad del juez o magistrado puede agravarse si a la falta anterior se suma la de no comunicar debidamente el fallo del sistema de IA a quien corresponde. El Reglamento IA regula un mecanismo que pretende frenar los efectos nocivos de un sistema de IA que esté funcionando incorrectamente, a fin de evitar cualquier daño a las personas. Y esto afecta también a la posible responsabilidad de los jueces y magistrados, en cuanto profesionales usuarios de los sistemas de IA de alto riesgo. Por ejemplo, en el caso de comprobar que los resultados contienen sesgos o que el sistema está dando lugar a errores, deben comunicarlo al proveedor en su condición de responsables del despliegue¹⁰⁰. En caso de incidente grave, no sólo están obligados a notificarlo al proveedor, sino al importador o distribuidor y a la autoridad de vigilancia del mercado correspondiente^{101, 102}. Si se omite esta comunicación y el sistema

⁹⁶ Artículo 32.1 LRJSP.

⁹⁷ Artículo 33.1 LRJSP, *a contrario sensu*.

⁹⁸ P. GALLO, «Nulidad de sentencia por uso de la IA: ¿crítica al fallo o miedo a la herramienta?», en *Almacén de Derecho*, 24 octubre 2025. La autora comenta brevemente una sentencia argentina del 15 de octubre de 2025, y contrasta la consulta hecha a la IA con las consultas que los jueces o magistrados pueden hacer con letrados, para señalar que unas y otras pueden influir en su proceso de toma de decisiones, sin que esto suponga infringir el principio del juez natural. A su juicio, la Cámara de lo penal de la provincia de Chubut cargó demasiado las tintas en el hecho de que no hubo transparencia, cuando realmente para anular la sentencia debiera haberse fijado en si el juez llegó o no a un fallo correcto. Sobre la impugnación de las resoluciones basada en el uso que se hizo de la IA, véase: M.J. ARIZA COLMENAREJO, «Impugnación de las decisiones judiciales dictadas con auxilio de inteligencia artificial», *Inteligencia artificial legal y Administración de Justicia*, S. Calaza López y M. Llorente Sánchez-Arjona (codirs.), Thomson-Reuters Aranzadi, 2022, pp. 29-54.

⁹⁹ En el considerando (27) RIA se explica que, conforme a *las directrices del Grupo independiente de expertos de alto nivel sobre IA*, se entiende por «acción y supervisión humanas» *que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, con respeto por la dignidad humana y la autonomía personal, y que el funcionamiento de los sistemas de IA se programa de manera que pueda ser controlada y vigilada adecuadamente por seres humanos*. El considerando (76) y (91) RIA, recogen la indicación del legislador de que los responsables del despliegue garanticen que quien se ocupe de la supervisión de los resultados tenga la competencia, *la formación y la autoridad necesarias* para desarrollar la función.

¹⁰⁰ En cuanto a los deberes de los responsables del despliegue en este sentido véase el artículo 26.5 RIA.

¹⁰¹ Al respecto, véase también lo dispuesto en el artículo 73.9 RIA.

¹⁰² Estos incidentes se gestionan de modo complejo -a efectos prácticos, desde la perspectiva que estamos abordando- pues deben notificarse a su vez por el proveedor a la autoridad correspondiente de vigilancia del mercado del Estado o Estados miembros en que se haya detectado el incidente, quien lo comunicará a las autoridades públicas nacionales responsables de velar por la protección de los derechos fundamentales, que están legitimadas para solicitar la documentación registrada o acceder a ella conforme a lo dispuesto en el Reglamento de IA, a fin de cumplir con su función, dentro de su jurisdicción [artículo 77.1, en relación con el artículo 17.i) RIA]. La notificación de un incidente grave (regulada en detalle, plazos incluidos, en el artículo 73 RIA), tiene como finalidades la evaluación de riesgos y la adopción de medidas que corrijan el defecto del sistema.

sigue produciendo errores, el juez o magistrado puede verse en la situación de asumir la responsabilidad no sólo en relación con el caso en que no lo advirtió, sino también -como corresponsable- en relación con casos posteriores operados por otros jueces o magistrados, que arrastren el mismo error.

IV. Perspectivas sociológica y psicológica, a modo de corolario.

40. Una vez analizados los aspectos éticos y jurídicos (en particular, las referencias del Reglamento IA a la cuestión), resulta interesante una breve aproximación, desde la sociología y la psicología, a modo de corolario. Pensemos cómo percibimos la justicia en el entorno digital. Si hiciéramos una encuesta sobre la confianza que merecen los sistemas de IA generados para realizar tareas *a imagen y semejanza* de las que son propias de los jueces y magistrados, probablemente encontraríamos argumentos contradictorios: De un lado, los optimistas tecnológicos afirmarían que a corto y medio plazo pueden alcanzarse resultados aceptables que agilicen el trabajo de los profesionales de la justicia, mientras que otros serán más reticentes y alegarán que la excesiva confianza en las máquinas redundaría en una pérdida de sentido crítico y reflexivo por parte de los profesionales, que pudieran relajarse con el consiguiente anquilosamiento de su agudeza para detectar los errores, cuando se produzcan, causando un perjuicio a las personas y al sistema en general. En el ámbito educativo, por ejemplo, ya se ha acreditado que un excesivo recurso a los medios digitales va en detrimento del correcto desarrollo del cerebro humano y se ha pasado del optimismo a la prudencia¹⁰³.

41. Lo anterior nos llevaría a desaconsejar el uso excesivo de la IA por parte de los jueces y magistrados, salvo que demos la vuelta a la consulta de partida y pongamos el acento en la percepción que tenemos de la justicia humana, ponderando si merece nuestra ciega confianza o si necesariamente será subjetiva y puede ser superada por la IA, más objetiva. A favor del uso de sistemas de IA en la toma de decisiones por parte de los profesionales, pudiera esgrimirse *la imperfección que deriva de la suma de los sesgos* que éstos pueden padecer, consciente o inconscientemente¹⁰⁴, pero no podemos olvidar que la IA funciona sobre la base de la anterior jurisprudencia y opiniones doctrinales, que a su vez estarían sesgadas y, por tanto, el argumento decaería: Los sistemas de IA pueden aprender a partir de datos que reflejan opiniones o decisiones sesgadas, dando lugar al *sesgo algorítmico* o *discriminación algorítmica*¹⁰⁵.

42. Aunque la calidad de los sistemas de IA es variada y existen sistemas muy perfeccionados en el sector legal, sería un craso error confiar al cien por cien en la veracidad o exactitud de los resultados arrojados por ellos (incurriendo -si se tratara de un juez- en un posible *sesgo de automatización*¹⁰⁶ o en un *sesgo de anclaje*¹⁰⁷), con independencia de lo muy precisos que sean, ya que los sistemas de IA

¹⁰³ Al respecto, véase: M. FERNÁNDEZ FERNÁNDEZ/A.M. SANCULESCU BUDEA/C.-M. FERNÁNDEZ ALAMEDA, «Retencencias desde la sociología y la comunicología ante el tecnooptimismo y la inteligencia artificial», *Tendencias sociales. Revista de sociología*, 2024-2(10), pp. 79-94.

¹⁰⁴ A.M. RODRÍGUEZ GUTIÁN, «Los sesgos y el derecho. En especial, sus implicaciones para el derecho civil», *InDret*, 2025.2, pp. 1-68, p. 5. La autora hace referencia a distintos tipos de sesgos que pueden padecer los profesionales: el sesgo del *status quo* (que llevaría, por ejemplo, a tomar una decisión conforme a lo ya establecido, en lugar de innovar); el sesgo de halo y de *horn* (según las conclusiones positivas o negativas de una persona se alcancen a partir de un determinado rasgo suyo); y el sesgo retrospectivo, que atribuye más en particular a los jueces, que llevará a predecir un resultado por la experiencia pasada, inconscientemente (*proyecta su nuevo conocimiento hacia el pasado*, explica la autora, p. 19). Por último, hace alusión al sesgo de género.

¹⁰⁵ F.M. SILVA ARDANUY, «Impacto de la discriminación directa e indirecta derivada del sesgo algorítmico en el ámbito de los derechos fundamentales: Alcance y protección constitucional», en *Inteligencia artificial y protección de datos. Desafíos en la era digital*, Colex, 2025, pp. 179-200. El autor explica que los sesgos algorítmicos reflejan los sesgos que los humanos tenemos *como personas y como sociedades*, y añade que la IA no distingue entre lo verdadero y lo falso, ni entre el bien y el mal, ni se rige por principios éticos (p. 192).

¹⁰⁶ El sesgo de automatización reduce de modo *inconsciente* la libertad del juez de alcanzar un resultado distinto del arrojado por el sistema de IA, como ha expresado M. DE ASÍS PULIDO, «Ética de la Inteligencia Artificial jurídica aplicada al proceso», *Cuadernos electrónicos de Filosofía del Derecho*, núm. 48, 2023, pp. 60-79, p. 75.

¹⁰⁷ M. BARRIO ANDRÉS [Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act), Francis Lefebvre, 2025, p. 109, 752 y 753, y pp. 131-132, 916 y 917] advierte de los riesgos que suponen las aplicaciones de la

pueden padecer *alucinaciones*, están hechos para responder de modo satisfactorio a las cuestiones que se plantean por lo que pueden dar respuestas contradictorias según los términos en que se produzca la consulta, o pueden dar injustificadamente -como hemos indicado- un trato distinto a casos iguales en función de factores discriminatorios con resultado contrario a Derecho.

43. Por la alta posibilidad de sesgos cognitivos como los apuntados -sesgo de automatización y sesgo de anclaje- y el riesgo de perjudicar la seguridad y los derechos fundamentales que ello supone en sectores especialmente críticos como es el desempeño de la función judicial, Moisés Barrio Andrés propone que el legislador nacional endurezca las medidas de supervisión previstas en el Reglamento IA, y respalda que el juez que utilice un sistema de IA como apoyo para dictar una sentencia o resolución, deba introducir su propuesta de sentencia al inicio, a fin de confirmarla o modificarla tras la consulta realizada, justificándolo¹⁰⁸. Muy críticos con la figura del juez-robot se han manifestado también, entre otros, Raúl Cancio Fernández, en un interesantísimo estudio¹⁰⁹, o Guillermo Cerdeira Bravo de Mansilla, quien destaca la incapacidad de la IA para detectar el problema jurídico¹¹⁰.

44. Consciente de ello, el mismo legislador europeo sale al paso con declaraciones de principios, al advertir que los conjuntos de datos empleados para uso de los sistemas de IA deben estar libres de errores, *en la mayor medida de lo posible*, para evitar injustas discriminaciones, prohibidas por el Derecho de la Unión, más aún cuando los datos de salida puedan influir en futuros datos de entrada (*bucles de retroalimentación*), como sucedería si se dictara sentencia sobre la base de datos anteriores erróneos, consolidando esos defectos del sistema con un impacto de potencial alcance. Los sesgos que existan en datos suministrados por el sistema *tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente*¹¹¹.

45. Por esta razón, en el Reglamento IA se impone a los proveedores y a los responsables del despliegue, la obligación de adoptar medidas de alfabetización en materia de IA, esto es, la obligación de impartir a los profesionales usuarios la formación necesaria para que tomen conciencia no sólo de las ventajas sino también de los daños que puede causar el uso de un concreto sistema de IA, o los riesgos que implica este uso¹¹². Y por esta razón, el único uso admitido de los sistemas de IA por parte de jueces y magistrados, cuando de tomar decisiones se trata, es el que requiere la necesaria supervisión humana, al considerarlos sistemas de alto riesgo.

V. Conclusiones

46. Desde la perspectiva ética, el uso de la IA como herramienta para el desempeño de la función judicial debe estar presidido por la primacía de la persona humana, su dignidad y los derechos que le son inviolables. Desde el punto de vista jurídico, esta centralidad de la persona humana es tenida en cuenta

IA que pueden preparar, por ejemplo, borradores de sentencias o resoluciones, ya que el juez puede padecer sesgos cognitivos tales como el sesgo de automatización y el sesgo de anclaje. El primero significa *que los usuarios de sistemas de asistencia automatizados no intervienen habitualmente si el sistema de asistencia no les incita a hacerlo*, incurriendo en errores por omisión, o bien *siguen las recomendaciones del sistema, aunque éstas contradigan su formación y otros indicadores disponibles*, incurriendo en errores por comisión. En cuanto al sesgo de anclaje, el autor explica que cuando las personas recibimos valores de referencia numéricos, está demostrado que tendemos a fiarnos de éstos, acortando *los procesos de pensamiento*. Cita para fundamentarlo la autoridad del premio Nobel Daniel Kahneman, *reconocido por su trabajo sobre la psicología del juicio humano y la toma de decisiones* bajo incertidumbre (cita completada con la fuente Wikipedia/Daniel Kahneman).

¹⁰⁸ M. BARRIO ANDRÉS, *Reglamento UE de inteligencia artificial (Incluye los actos de desarrollo y ejecución de la AI Act)*, Francis Lefebvre, 2025, pp. 132-133, 923.

¹⁰⁹ R.C. CANCIO FERNÁNDEZ, «¿Sueñan los jueces con sentencias electrónicas?», *Revista Análisis Jurídico-Político*, vol. 2, n° 3, 2020, pp. 145-168.

¹¹⁰ G. CERDEIRA BRAVO DE MANSILLA, «La deshumanización del arte jurídico: El llamado juez-robot: ¿mito o realidad?», *Actualidad jurídica iberoamericana*, N. 23, agosto 2025, pp. 14-51, pp. 38-41.

¹¹¹ Considerando (67) RIA. Véase también el considerando (70) RIA.

¹¹² Artículo 4 RIA, en relación con la definición del artículo 3.56) RIA.

por el legislador europeo en el Reglamento (UE) 2024/1689, de IA, y tiene dos importantes consecuencias inmediatas: La prohibición de los sistemas de IA que tomen decisiones que afecten directamente a la salud, seguridad o derechos fundamentales de los ciudadanos, y la declaración como sistemas de alto riesgo de aquéllos que ayuden a los profesionales en el proceso de toma de decisiones que puedan afectar a los ciudadanos en lo que se refiere a su salud, seguridad o derechos fundamentales.

47. La puesta en el mercado de sistemas de IA de alto riesgo, requiere que estos cumplan los requisitos de calidad, transparencia, trazabilidad y necesaria supervisión humana, entre otros, que serán controlados conforme dispone la UE. A la vez, el proveedor y los responsables del despliegue tomarán medidas para lograr la alfabetización de los profesionales usuarios de los sistemas de alto riesgo, esto es, su formación con vistas a garantizar que la salud, seguridad y derechos fundamentales de las personas no sufra menoscabo por un mal uso de estos sistemas (por ejemplo, por un exceso de confianza en la exactitud, actualización o veracidad de los resultados que arrojen).

48. Los jueces y magistrados pueden hacer uso de los sistemas de IA de alto riesgo bajo su personal responsabilidad (penal, disciplinaria y civil). Son sistemas de IA de alto riesgo los destinados a apoyar al juez o magistrado en el proceso de toma de decisiones, y, por tanto, los que son capaces de suministrar el borrador de una resolución judicial. El juez o magistrado deberá en todo caso hacer un buen uso de la IA, lo que requiere supervisar críticamente cada resultado que obtenga de ella. La supervisión debe ser real y eficaz. La mera supervisión formal, clicando la casilla correspondiente, no sólo no exonera de responsabilidad, sino por el contrario, señala al sujeto responsable en caso de dictarse una sentencia injusta que cause daño a tercero. La supervisión por un juez o magistrado es suficiente, salvo cuando se haya alcanzado un resultado empleando un sistema de identificación biométrica remota, que requiere un mínimo de dos supervisores. Conforme al Reglamento IA, los jueces y magistrados deberán informar a los terceros que puedan resultar afectados sobre el uso que se ha hecho de los sistemas de IA de alto riesgo para alcanzar el resultado (transparencia). En España, sólo se admite que los jueces y magistrados utilicen en el desempeño de sus funciones sistemas de IA facilitados por la Administración competente o por el CGPJ.