

1. POLÍTICA DE USO DE LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN DE JUSTICIA.....	3
1.1 OBJETIVO.....	3
1.2 AMBITO DE APLICACIÓN.....	3
1.3 DESTINATARIOS.....	3
1.4 PRINCIPIOS BÁSICOS QUE ORIENTAN ESTA POLÍTICA DE USO.....	4
1.5 NORMAS DE USO DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL.....	6
1.6 RESPONSABILIDADES Y CONTROL DE LA IA.....	7
2. ANEXO I: DEFINICIONES.....	8
3. ANEXO II: CASOS DE USO PERMITIDOS Y PROHIBIDOS.....	10

1. POLÍTICA DE USO DE LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN DE JUSTICIA

1.1 OBJETIVO

En los últimos años, se están desarrollando e implementando diversas herramientas de inteligencia artificial, tanto en el sector privado como en el ámbito público, incluyendo también a la propia Administración de Justicia. Así, y en consonancia con esta realidad, el Real Decreto-ley 6/2023, de 19 de diciembre, ha introducido en su Capítulo VII las actuaciones automatizadas, proactivas y asistidas, en sus artículos 56, 57 y 58, de los cuales se deriva el posible uso de la inteligencia artificial en el apoyo de las actuaciones jurisdiccionales.

Este uso por parte de los juzgados y tribunales, garantes de la tutela judicial efectiva, debe dar cumplimiento a lo establecido en el Reglamento de Inteligencia Artificial, a la normativa de protección de datos personales y las normas procesales. Todo esto conlleva a que se deban adoptar unos criterios mínimos, tanto por aquellos que van a impulsar este tipo de proyectos como por los propios usuarios.

En consecuencia, a través de este documento se fijan una serie de criterios mínimos con la finalidad de asegurar un uso responsable, legal y ético de la Inteligencia Artificial en el ámbito de la Administración de Justicia, incluyendo un Anexo con definiciones, así como un desglose de usos aceptados y otros prohibidos.

1.2 AMBITO DE APLICACIÓN

Esta Política se aplica a cualquier sistema o servicio que se nutra de datos judiciales, considerando éstos como cualquiera que sea producido en el marco de un procedimiento judicial, desde la presentación del primer escrito o demanda hasta la resolución judicial final, incluyendo también las posibles publicaciones o notificaciones de los expedientes.

A los efectos de determinar las correspondientes responsabilidades, que más adelante se detallan, será necesario diferenciar el uso de aquellas herramientas de inteligencia artificial que puedan afectar a la actividad propiamente jurisdiccional, y, por consiguiente, afectar a la independencia judicial, de aquellos que no afectan.

Además, ese uso de datos judiciales, si supone un tratamiento de datos personales, conlleva un tratamiento de datos jurisdiccionales, por afectar a la actividad jurisdiccional de juzgados y tribunales.

1.3 DESTINATARIOS

Todos los trabajadores de la Administración de Justicia deben respetar el contenido de esta Política, teniendo que ser ratificada su adopción de manera específica por parte del Consejo General del Poder Judicial (CGPJ), Fiscalía General del Estado (FGE), Comunidades Autónomas con competencias en materia de Justicia y Ministerio de la Presidencia, Justicia y Relaciones con las Cortes (MPJRC).

También debe ser respetada por el personal al servicio de **proveedores de herramientas de inteligencia artificial**, así como a **cualquier otro actor institucional, público o privado**, que tenga acceso a la información que obre en poder de las administraciones con

competencias y CGPJ, o se encuentre alojada en los sistemas destinados a la Administración de Justicia.

1.4 PRINCIPIOS BÁSICOS QUE ORIENTAN ESTA POLÍTICA DE USO

El CEPEJ (“European Commission for the Efficiency of Justice”) en su sesión plenaria del 3-4 diciembre de 2018, adoptó el documento denominado “European ethical charter on the use of Artificial Intelligence in judicial systems and their environment”, que contempla cinco principios básicos que deben cumplirse.

Estos principios son los siguientes:

1. **Principio de respeto a los derechos fundamentales:** cuando se utilicen herramientas de inteligencia artificial para resolver un litigio o para la ayuda de toma de decisiones judiciales, se debe garantizar la tutela judicial efectiva, la independencia judicial y un proceso basado en la equidad entre las partes.

En consecuencia, el desarrollo de estas herramientas procede realizarse aplicando la ética y el respeto de los derechos humanos en su diseño.

Además, la IA nunca debe reemplazar la toma de decisiones humanas en cuestiones cruciales de la Administración de Justicia. Es fundamental que los sistemas de IA se utilicen como herramientas para ayudar a los profesionales del derecho en sus funciones, pero la responsabilidad final de tomar decisiones legales debe recaer en jueces y magistrados. Se debe asegurar su toma de decisión de forma independiente.

2. **Principio de no discriminación:** conlleva que se tenga que garantizar que no se produzca la misma. Supone que tanto en el desarrollo como aplicación de la inteligencia artificial no se produzca discriminaciones en base al uso de información especialmente sensible como pueden ser datos de origen racial, étnico, socioeconómico, opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos, datos genéticos, datos biométricos, datos de salud, relativos a la vida sexual u orientación sexual.

De esta forma, desde el aprendizaje de estos sistemas se debe orientar a que no se produzca esta discriminación.

3. **Principio de calidad y seguridad:** para un correcto desarrollo se debe aprovechar la experiencia de los profesionales en general, como serían jueces/zas, magistrados/as, fiscales, así como investigadores/as y profesores/as de otros campos tanto del Derecho como de las Ciencias Sociales o de la propia ingeniería, y conseguir con ello un enfoque multidisciplinar, compartiéndolas entre todas las salvaguardas éticas.

También implica el uso de fuentes certificadas, que no serán modificadas hasta que hayan sido utilizadas en el mecanismo de aprendizaje, siendo todo el proceso rastreable a fin de que no se produzca ninguna modificación.

Tanto los modelos como algoritmos creados se almacenarán y ejecutarán en entornos seguros, para garantizar la integridad del sistema y su intangibilidad.

4. **Principio de respeto a la transparencia, imparcialidad y lealtad:** de manera que el desarrollo de estos sistemas sea accesibles, entendibles y auditables.

Para ello debe conseguirse un equilibrio entre la propiedad intelectual y el cumplimiento de estos principios de transparencia, imparcialidad, equidad y lealtad, para que se permita el acceso al diseño de estos sistemas, no se produzcan sesgos, y se priorice los intereses de la Justicia.

Los algoritmos utilizados en la Administración de Justicia deben ser transparentes y explicables. Los ciudadanos tienen derecho a comprender cómo se toman las decisiones que afectan sus vidas, especialmente cuando se trata de procesos judiciales. Se deben implementar medidas para garantizar que las decisiones automatizadas sean comprensibles y puedan ser examinadas por expertos y partes interesadas. Es altamente recomendable ofrecer publicidad y transparencia a través de los sitios web oficiales de miembros del CTEAJE. Concretamente, es deseable la publicación de los registros FAT (Fairness, Accuracy and Transparency) o instrumentos similares, acerca de los datos usados, miembros de los equipos de IA, servicios, algoritmos, posibles sesgos y aplicaciones que hacen uso de técnicas de inteligencia artificial.

Podrá valorarse el uso de los servicios de IA de última generación que, por motivos derivados de lo novedoso o puntero de su tecnología no sean capaces de ofrecer una elevada explicabilidad, siempre que no supongan un menoscabo en los derechos de los justiciables, o en las propias funciones jurisdiccionales y sean plenamente conformes con el régimen normativo aplicable.

5. **Principios bajo control del usuario:** supone que, aunque se use un sistema de inteligencia artificial, debe garantizarse que las decisiones judiciales pueden ser revisadas previamente.

También habrá que informar a los ciudadanos que puedan verse afectados por el sistema, en un lenguaje claro y comprensible si los resultados que ofrece la herramienta son vinculantes o no, así como su posible uso durante el procedimiento judicial, antes o durante el mismo, y su derecho a objetar de manera que pueda ser oído directamente por un órgano judicial.

Además de estos principios impulsados por el CEPEJ, también se deben respetar los siguientes:

1. **Principio de Equidad y Acceso Universal:** La IA en la Administración de Justicia debe ser utilizada para garantizar un acceso equitativo a los sistemas judiciales, independientemente de la ubicación, el estatus socioeconómico o cualquier otra característica demográfica. Esto implica desarrollar soluciones que eliminen barreras y aseguren que todos los ciudadanos tengan la misma oportunidad de hacer valer sus derechos ante la ley.
2. **Principio de Prevención de Sesgos y Discriminación:** La IA en la Administración de Justicia debe ser diseñada para evitar sesgos y discriminación. Es fundamental realizar evaluaciones periódicas de los algoritmos para identificar y corregir posibles

sesgos inherentes a los datos de entrenamiento o algoritmos utilizados. Además, se deben establecer salvaguardas para proteger los derechos de las personas y evitar la perpetuación de injusticias sistémicas.

3. **Principio Protección de la Privacidad y Datos Personales:** Se deben establecer estrictas medidas de protección de la privacidad y los datos personales en el uso de la IA en la Administración de Justicia, incluyendo la necesidad de realizar con carácter previo evaluaciones de impacto de la protección de datos. Los sistemas deben cumplir la normativa de protección de datos existente y garantizar que la información confidencial de los individuos se maneje de manera segura y ética.
4. **Principio de Innovación Responsable y Evaluación Continua:** Se debe fomentar la innovación responsable en el desarrollo y la implementación de la IA en la Administración de Justicia. Esto implica realizar evaluaciones periódicas del impacto de la tecnología en el sistema judicial y estar dispuestos a realizar ajustes y mejoras según sea necesario para garantizar su efectividad y equidad.
5. **Principio Formación y Capacitación:** Es fundamental proporcionar formación y capacitación adecuadas a los profesionales del derecho y otros actores involucrados en el uso de la IA en la Administración de Justicia. La comprensión de los principios éticos y prácticos relacionados con la IA es esencial para garantizar su uso responsable y efectivo.
6. **Principio de Cogobernanza:** Se ha de fomentar la colaboración, compartiendo e intercambiando conocimientos, así como los propios sistemas basados en IA entre diferentes áreas de la organización, o con el resto de las administraciones con competencias en materia de Justicia, el CGPJ, y la FGE o con otras instituciones, de tal forma que se impulse el deseado desarrollo innovador en sintonía con una implementación ética de la inteligencia artificial.

1.5 NORMAS DE USO DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

El uso de la IA en la Administración de Justicia debe cumplir en todo momento las diferentes normativas, tanto europea como nacional, que le sea aplicable.

De forma general hay que tener en cuenta que:

1. La revisión humana de todo lo generado siempre que afecte de manera directa o indirecta a los derechos de las personas usuarias del servicio público de Justicia o a la propia actividad jurisdiccional.
2. La soberanía del dato y de la información debe ser siempre protegida y respetada. Ni el dato/información de origen ni el generado debe estar nunca accesible a terceros (no autorizados).
3. Debe revisarse que no existe sesgo en las herramientas.
4. Todos los resultados obtenidos de la IA generativa deben identificarse como generados por una IAGen.
5. No utilizar aplicaciones de IA que no hayan sido autorizadas.

6. No instalar interfaces de programación de aplicaciones (API), complementos, conectores o software no aprobados relacionados con los sistemas IA.
7. Deben revisarse los resultados de las aplicaciones de IA para asegurarse de que cumplen con los estándares de la organización en cuanto a principios de equidad, ética e idoneidad.
8. No utilizarse ningún resultado que discrimine a las personas por motivos de raza, color, religión, sexo, origen nacional, edad, discapacidad, estado civil, afiliación política u orientación sexual.
9. No utilizarse las aplicaciones de IA para crear contenido de texto, audio o visual con el fin de cometer fraude o para tergiversar la identidad de una persona o la comisión de cualquier otro acto ilícito.

1.6 RESPONSABILIDADES Y CONTROL DE LA IA

Deben determinarse las diferentes responsabilidades que conlleva la IA en la Administración de Justicia. Así, se puede diferenciar entre:

Con relación al **uso de la IA**: el responsable de su uso será el juzgado, tribunal, oficina judicial o fiscalía, y dentro de cada uno de ellos, la persona que realice una utilización de efectiva. Asimismo, en los servicios ofrecidos a la ciudadanía o a los profesionales de la Justicia, lo será la propia persona usuaria del mismo.

Con relación al **desarrollo e implementación de sistemas de IA**, la Administración prestacional correspondiente.

Con relación al **control de calidad de la IA y auditoría**. Dependerá de:

- Si afecta al ejercicio de la función jurisdiccional, y, por consiguiente, a la independencia judicial, le corresponde, conforme a la LOPJ, al Consejo General del Poder Judicial. La vigilancia algorítmica de los sistemas susceptibles de afectar a la independencia judicial requerirá por parte del CGPJ de la recopilación y análisis de datos generados por algoritmos para evaluar su desempeño, identificar posibles sesgos, errores o comportamientos no deseados, y garantizar la transparencia y responsabilidad en el uso de la inteligencia artificial.
- Si no afectase, le corresponde, conforme al RD Ley 6/2023, al CTEAJE o a la administración prestacional, según el ámbito de aplicación de dicho sistema.

2. ANEXO I: DEFINICIONES

1. **La inteligencia artificial (IA):** Sistema diseñado para funcionar con un cierto nivel de autonomía y que, basándose en datos de entradas proporcionadas por máquinas o por personas, infiere cómo lograr un conjunto de objetivos establecidos utilizando estrategias de aprendizaje automático o basadas en la lógica y el conocimiento, y genera información de salida, como contenidos (sistemas de inteligencia artificial generativos), predicciones, recomendaciones o decisiones, que influyan en los entornos con los que interactúa.
2. **La IA generativa (IAGen):** Se refiere a una tecnología de inteligencia artificial que deriva nuevas versiones de texto, audio o imágenes visuales a partir de grandes cantidades de datos en respuesta a las indicaciones del usuario. IAGen se puede utilizar en aplicaciones independientes, como ChatGPT o Bard, o incorporado en otras aplicaciones¹. Además, las propias administraciones pueden poner a disposición sistemas de este tipo.
3. **"Alucinaciones":** Se ha convertido en el término adoptado por la comunidad IAGen para describir cómo los modelos, de vez en cuando, proporcionarán respuestas ficticias. El problema no es simplemente que las respuestas sean incorrectas, sino que son seguras y convincentes. La sociedad ha desarrollado un sesgo de automatización endémico, los humanos favorecen ciegamente las sugerencias de los sistemas automatizados de toma de decisiones, a menudo ignorando su propio mejor juicio.
4. **Ciberseguridad:** La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa.
5. **Confianza y privacidad:** La información confidencial y sensible, incluidos los datos personales de clientes, empleados u otros, ingresados en aplicaciones IAGen disponibles públicamente, puede dejar residuos dentro del modelo que pueden formar parte de un resultado en otro lugar después, o usarse para (re) entrenar nuevos modelos. Por lo tanto, cualquier información personal, información de propiedad o propiedad intelectual, o información confidencial ingresada en el mensaje puede aparecer en la salida de otros usuarios.
6. **Sesgo del modelo:** Las herramientas IAGen incorporan cualquier sesgo de los conjuntos de datos que se utilizaron para entrenarlos. Este sesgo de modelado no siempre se alinea con el valor central de la Administración de Justicia y su compromiso con la diversidad, la equidad y la inclusión. Por lo tanto, la salida del modelo puede cometer errores sistemáticos o favorecer a ciertos grupos, lo que lleva a resultados injustos o discriminatorios.
7. **Propiedad intelectual:** Los modelos IAGen a menudo se entrenan en grandes conjuntos de datos disponibles públicamente (por ejemplo, a través de la extracción de datos de páginas web públicas). Por lo tanto, los resultados pueden contener información protegida por derechos de autor o propiedad intelectual de otros. Si bien la propiedad en muchos de estos casos no está clara, los usuarios deben pecar de

¹ Como Microsoft Bing o Microsoft Office Suite.

- cautelosos y no utilizar ningún resultado que contenga material que sospechen que está bajo protección de derechos de autor en ningún material, interno o externo.
8. **Riesgo de transparencia:** Todo el contenido generado utilizando IAGen debe estar claramente identificado en cualquier contenido orientado hacia el exterior.
 9. **Riesgo de terceros:** Los datos enviados por las administraciones a terceros podrían utilizarse en el uso de herramientas IAGen por parte de estos actores externos a la Administración de Justicia. Por ejemplo, la información confidencial del usuario es un riesgo potencial si la organización utiliza un proveedor externo de chatbot de servicio al cliente que emplea herramientas IAGen.
 10. **Algoritmo:** Es un conjunto de instrucciones o reglas definidas que se utilizan para realizar una tarea o resolver un problema específico. Los algoritmos son la base de muchos sistemas de IA, ya que permiten que las máquinas aprendan y tomen decisiones.
 11. **Aprendizaje Automático (Machine Learning):** Es una subdisciplina de la IA que se centra en el desarrollo de algoritmos y modelos que permiten a las computadoras aprender patrones y realizar predicciones a partir de datos, sin necesidad de ser programadas explícitamente para cada tarea.
 12. **Redes Neuronales Artificiales (ANN):** Son modelos computacionales inspirados en el funcionamiento del cerebro humano que se utilizan en el aprendizaje automático y otros campos de la IA. Están formadas por nodos interconectados (neuronas) que procesan información y pueden adaptarse mediante el ajuste de los pesos de las conexiones entre ellas.
 13. **Aprendizaje Profundo (Deep Learning):** Es una técnica de aprendizaje automático que utiliza redes neuronales artificiales con múltiples capas de procesamiento para aprender representaciones de datos de forma jerárquica. El aprendizaje profundo ha demostrado ser muy efectivo en tareas como el reconocimiento de imágenes, el procesamiento de lenguaje natural y la conducción autónoma.
 14. **Robótica Inteligente:** Es un campo de la IA que combina la inteligencia artificial con la robótica para desarrollar sistemas robóticos capaces de percibir su entorno, tomar decisiones autónomas y realizar tareas de manera eficiente. La robótica inteligente se aplica en una amplia gama de áreas, desde la manufactura hasta la exploración espacial.

3. ANEXO II: CASOS DE USO PERMITIDOS Y PROHIBIDOS

Todo uso de IA, mientras se realiza un trabajo para cuestiones laborales relacionados con la Administración de Justicia, está sujeto a la aprobación de la dirección. A continuación, se muestran ejemplos de casos de uso que están sujetos a modificaciones. La siguiente tabla no refleja todos los casos y escenarios de uso posibles. Usa tu mejor juicio y haz preguntas.

CATEGORÍA	CASOS DE USO Y EJEMPLOS	ACCIONES NECESARIAS
<p>Casos de uso generalmente permitidos</p>	<p>Los usos que no involucran información personal o información confidencial son solo para una audiencia interna y cuyo resultado no se utilizará en resoluciones judiciales o administrativas.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> - Traducción de texto de una fuente secundaria disponible públicamente. - Llevar a cabo una investigación de antecedentes de alto nivel sobre un tema no delicado. - Generación de informes que no afectan a derechos u obligaciones de los ciudadanos. - Obtener resúmenes de documentos extensos, en forma de texto, vídeo o audio. 	<p>Siempre compruebe si el servicio utilizado es prestado por la administración o algún organismo confiable de acuerdo con este protocolo, para tomar una decisión sobre su posible uso.</p> <p>Revise los resultados para asegurarse de que se ajusten a las directrices de la organización.</p> <p>Recuerda que los datos generados pueden no ser precisos ni completos, por lo que los resultados deberán ser revisados y la lectura de los documentos no está eximida si la norma así lo exige.</p> <p>Los datos sobre los que trabaja la IA no pueden ser usados cuando sean específicamente datos personales o confidenciales, pero, además, recuerde que también puedan contener información que permitiera inferir la identificación de personas o en general, comprometer información, a través de otros datos (Ejemplos: el vecino de la calle X, 4ºB, de Madrid. O el vecino del pueblo X conocido como "perico").</p>

<p>Casos de uso que requieren la aprobación de la dirección</p>	<p>Aquellos que, en el caso anterior (sin datos con algún tipo de protección), puede ser usado para atender a los ciudadanos, profesionales o empresas, con los datos propiamente aportados por estas personas.</p> <p>Aquellos que, en el caso anterior (sin datos con algún tipo de protección), usan información que será utilizada para la toma de decisión.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> - Texto generado para material informativo, promocional o formativo. - Cuando la salida se utiliza en informes o documentos, en general, que tienen como destinatarios los ciudadanos, profesionales o empresas. <p>Aquellos que, usando datos privados, personales, confidenciales, o en general, con algún tipo de protección, pueden aportar resultados que sean necesarios para el desarrollo y como apoyo de la actividad que le es propia a la organización, siendo el servicio provisto por la propia administración o específicamente aprobado por el departamento de seguridad:</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> - Determinados informes que afectan a la intimidad de las personas, o aquellos que son tratados en el ámbito de las investigaciones judiciales, tales como la textualización en escuchas telefónicas, resúmenes de las mismas, etc. - Informes de soporte y ayuda en temas de jurisprudencia, u otros similares. - Generación de imágenes y videos a partir de información. Podría utilizarse para reconstrucción de escenarios en declaraciones. 	<p>Ha de solicitar formalmente la petición a sus responsables, y ha de obtener una o las autorizaciones explícitas.</p> <p>Ha de informar al departamento de seguridad, además de a la administración encargada de la innovación en la IA, para que el servicio sea publicado, en su caso, en los registros FAT.</p>
--	--	--

	<ul style="list-style-type: none"> - Elaboración de resúmenes y descripción de imágenes y videos. Podría utilizarse como apoyo al análisis de evidencias de difícil percepción por el ojo humano, como el análisis de tejidos, detección de patrones en imágenes, etc. - Generación de borradores de documentos. - Simplificación de textos jurídicos a lenguaje sencillo. 	
<p>Casos de uso que requieren aprobación de TI</p>	<p>Generar código que se ejecutará en cualquier dispositivo de la organización.</p>	<p>Realice una revisión por pares del código y póngase en contacto con el departamento de seguridad para su aprobación.</p>
<p>Prohibido</p>	<p>Uso de datos de carácter personal o con algún tipo de protección cuyo uso no se encuentra en los casos anteriores. Específicamente, usar documentos y datos protegidos para generar información o documentos para la toma de decisiones que afectan a derechos u obligaciones de los ciudadanos, profesionales o empresas, si bien se permite previa autorización, la generación de documentación de soporte que sea usada en expedientes judiciales o en el ámbito de toma decisiones de la administración.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> - Obtener informes para la toma de decisión judicial o administrativa en base a datos aportados por el usuario. - Generación de resoluciones definitivas que serán automáticamente emitidas. - Informar de manera automatizada del estado y detalle de los procedimientos a los interesados en 	<p>Por favor, informe de cualquier uso prohibido de los modelos IAGen al departamento de seguridad.</p>

	<p>él, sin una supervisión humana previa.</p> <ul style="list-style-type: none"> - Generación de documentación o información de soporte sobre la previsible conducta futura de las personas para basar en ella la actuación judicial basada en sus antecedentes personales o de personas de características similares (ej: no dictar una prisión provisional o una libertad condicional basado en un informe de recomendaciones de IA) <p>El uso de sistemas de inteligencia artificial generativa que sustituya la irremediable presencia en comités, reuniones, o similares.</p> <p>Ejemplo:</p> <ul style="list-style-type: none"> - Uso de sistemas que procesan el audio de las reuniones y realizan resúmenes automáticos puede llevar a los usuarios a no acudir a las mismas. 	
--	---	--