

Decálogo

para el uso responsable de la IA
en Administraciones Públicas

PREÁMBULO

La introducción de tecnologías que hacen uso de la Inteligencia Artificial (IA) es una realidad tanto para el sector público como para el sector privado. Como consecuencia de ello, la Unión Europea, mediante la adopción del Reglamento de Inteligencia Artificial (en adelante, Ley de IA), pretende establecer un marco jurídico que garantice sus posibles usos respetando en todo momento los derechos de los ciudadanos y la legalidad vigente.

Así mismo, la evolución de las normas reguladoras de la actividad de las Administraciones Públicas (AAPP) se ha caracterizado en los últimos años por buscar los procesos eficientes, transparentes, ágiles y centrados en el servicio a los ciudadanos y las empresas, impulsando medidas para racionalizar la actuación administrativa, mejorar la eficiencia en el uso de los recursos públicos y aumentar su productividad.

Una de las adaptaciones que la introducción de las tecnologías ha permitido integrar en la actividad de las AAPP ha sido la actuación administrativa automatizada definida, en su artículo 41, por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público como *“cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público”*. En estos casos, según la norma, corresponde a la Administración establecer previamente el órgano u órganos competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente, así como la indicación del órgano que debe ser considerado responsable a efectos de impugnación. Aunque no puede decirse que toda actuación administrativa automatizada conlleve el uso de IA, a buen seguro, será en este ámbito uno de los cuales el uso de sistemas de IA por las AAPP tendrá una mayor repercusión.

Otro ámbito en el que, no cabe duda, que la IA tiene repercusión es en el relativo al derecho fundamental a la protección de datos, para lo cual, las AAPP deberán incorporar la normativa de protección de datos al cumplimiento de la Ley de IA en la medida en que el diseño, el desarrollo, el entrenamiento o el uso de sistemas de IA de dichas AAPP implique el tratamiento de datos personales, ya actúen como responsables o encargados del tratamiento.

Además, no son pocas normas las que están introduciendo obligaciones en el uso de sistemas de IA en el ámbito del sector público.

Así, por ejemplo, la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que en su artículo 23 *“Inteligencia Artificial y mecanismos de toma de decisión automatizados”* exige a las AAPP promover la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las AAPP tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente, bajo la realización previa de evaluaciones de impacto el posible sesgo discriminatorio, priorizando la transparencia en el diseño y la implementación así como la capacidad de interpretación de las decisiones adoptadas por los algoritmos utilizados. Así mismo, esta norma anima a que las AAPP promuevan el uso de una IA ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido y promoviendo un sello de calidad de los algoritmos.

Otro ejemplo de ello es la Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana que, en su artículo 16.1 I), exige publicar a las AAPP valencianas la *“relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad”*.

En virtud de todo lo anterior se presenta un **DECÁLOGO SOBRE EL USO DE LA INTELIGENCIA ARTIFICIAL POR LAS ADMINISTRACIONES PÚBLICAS** que estas pueden tener en cuenta para favorecer el cumplimiento de sus obligaciones en cuanto al uso de sistemas de IA en el desarrollo de su actividad, sin perjuicio de cualesquiera buenas prácticas que, además, las AAPP deseen adoptar.

DECÁLOGO

1.- Política de gobernanza: establecimiento de un modelo de gobernanza integral para administrar y supervisar las prácticas y actividades de IA que incluya tanto personas con capacidades y competencias como medidas para garantizar la ética, seguridad, equidad, transparencia, protección de datos y la legalidad vigente. Esta política deberá incluir, entre otras, las siguientes cuestiones:

- **Gestión integral del ciclo de vida de la IA:** Inclusión de todas las fases de la IA donde se diseñen o produzcan tratamientos de datos personales, desde el diseño del modelo de datos, pasando por el entrenamiento del algoritmo hasta su implementación y uso final, y posteriormente su retirada. Deberá

especificarse las bases legitimadoras aplicables, y si fuese necesario, la que corresponde a cada fase, ajustándose a las necesidades y requisitos legalmente aplicables.

- **Creación de un Equipo de trabajo multidisciplinar:** Formar un equipo de trabajo para el análisis de la IA desde una perspectiva técnica, ética y legal. Este equipo debe incluir al delegado de protección de datos de la administración responsable, asegurando una supervisión adecuada y continua.
- **Regulación de los usos prohibidos de la IA:** Determinar la prohibición de determinados usos de sistemas de IA, en función de las finalidades o datos involucrados, que deberá incluir las prácticas catalogadas como prohibidas por la Ley de IA con las salvedades y excepciones para las situaciones y con las condiciones previstas en la propia Ley.
- **Metodologías para evaluar y gestionar el riesgo del sistema de IA:** Desarrollar y adoptar metodologías para evaluar los riesgos asociados a los sistemas de IA, asegurando que se identifiquen y se gestionen de forma que se mitiguen los posibles impactos negativos.
- **Implementación de procesos para aplicar los principios de transparencia y explicabilidad de la IA** tanto desde la perspectiva de la normativa relativa a la IA como desde la perspectiva del RGPD.
- **Aplicación del principio de responsabilidad proactiva:** todas las fases y medidas mencionadas deben ser documentadas por la AAPP y periódicamente controladas y auditadas con el fin de acreditar y demostrar frente a las autoridades de control y supervisión el cumplimiento legal, conservando la documentación correspondiente al efecto.

2. Adecuación de los procesos de contratación pública a las exigencias de la Ley de IA: Lo que conlleva, al menos, la necesidad de dar cumplimiento a las siguientes cuestiones:

- **Cumplimiento de obligaciones:** Requerir a los proveedores de sistemas de IA la entrega de una declaración responsable que de forma expresa manifieste el cumplimiento de todas sus obligaciones contempladas en la Ley de IA. Esto incluye asegurar que el producto ofrecido cumpla con los requisitos específicos de la administración pública contratante.

- **Documentación y certificación:** Los proveedores deberán proporcionar la documentación técnica y certificados que demuestren el cumplimiento de las normativas aplicables. Esta documentación también deberá incluir criterios de transparencia y explicabilidad conforme a las normativas tanto europeas como nacionales.
- **Competencia del personal:** Los proveedores deben presentar una declaración responsable que manifieste la garantía de un nivel suficiente de conocimientos de IA de su personal y de otras personas que se ocupen del funcionamiento y uso de los sistemas de IA en su nombre, teniendo en cuenta sus conocimientos técnicos, experiencia, educación y formación y el contexto en el que vayan a utilizar los sistemas de IA por la AAPP contratante.
- **Responsabilidades contractuales:** En la documentación contractual se detallará con claridad las funciones, obligaciones y responsabilidades tanto del proveedor como de la AAPP contratante. Esto es fundamental para garantizar el cumplimiento de las disposiciones relativas a las pruebas en condiciones reales con arreglo a la Ley de IA y otros actos legislativos de la Unión y nacionales aplicables.
- **Inclusión de Expertos en Protección de Datos:** Será recomendable que se incluya un experto legal en protección de datos e IA, entre el personal técnico o unidades técnicas, integradas o no en la empresa, que participen en el contrato, sin perjuicio de aquellos supuestos en que sea obligatorio contar con la persona del delegado de protección de datos conforme al Reglamento General de Protección de Datos (RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

3.- Capacitación, formación y concienciación de los empleados/as públicos como usuarios de los sistemas de IA:

Las AAPP tomarán medidas para garantizar que tanto su personal como cualquier otra persona involucrada en el funcionamiento y uso de los sistemas de IA en su nombre, posean un conocimiento adecuado sobre estas tecnologías. Esta capacitación tendrá en cuenta los conocimientos técnicos, la experiencia previa, la educación y la formación de cada individuo, así como el contexto específico en el que se emplearán los sistemas de IA y los grupos de personas afectados por su uso.

Esta formación asegurará el conocimiento y entendimiento por los empleados/as públicos de las normas legales y políticas internas que afectan al cumplimiento

normativo de los sistemas de IA en la entidad.

4.- Análisis y gestión de riesgos y, en caso desplegar sistemas de IA de alto riesgo, evaluación de impacto en los derechos fundamentales, de forma previa al uso de los sistemas de IA con superación de los correspondientes juicios de proporcionalidad, ético, legal y técnico (o de seguridad) y determinación de las medidas y estrategias de mitigación del riesgo; en el supuesto de que sea legalmente exigible, se notificará los resultados de la evaluación de impacto a la autoridad de vigilancia del mercado.

5.- Categorización de los sistemas de IA según los niveles de riesgo establecidos en la Ley de IA y elaboración de un inventario de sistemas de IA utilizados: Las AAPP deben clasificar y registrar todos los sistemas de IA que utilizan, siguiendo los niveles de riesgo establecidos en la Ley de IA. Este proceso incluirá la creación de un inventario detallado que identifique cada sistema según su nivel de riesgo —alto, limitado o mínimo—, y describa su impacto en los procedimientos administrativos o la prestación de servicios públicos. Además, el inventario proporcionará una descripción clara y comprensible del diseño y funcionamiento de cada sistema, así como información de contacto pertinente, con el fin de garantizar la transparencia y la explicabilidad. Esta categorización y registro se realizarán en consonancia con el Esquema Nacional de Seguridad (ENS), y cumplirán con todas las obligaciones específicas relacionadas con el uso de sistemas de IA.

En el caso de que se produzcan incidentes graves se procederá a su notificación a las autoridades de control y supervisión que corresponda.

6.- Transparencia de los sistemas de IA: Todos los sistemas de IA deben estar documentados y ser transparentes de forma que las partes interesadas conozcan cómo funcionan los algoritmos, de qué tipo son (predicción y decisión automatizada o de soporte a la decisión) y el impacto que tiene sobre las personas (explicabilidad o transparencia algorítmica o el derecho a la explicación). La transparencia de los sistemas de IA se integrará, cuando afecten a datos personales, con las obligaciones del RGPD a través, principalmente, de los registros de las actividades de tratamiento y el cumplimiento del deber de información.

Así mismo, cuando corresponda, las AAPP deben proporcionar explicaciones

claras y significativas sobre el papel que los sistemas de IA de alto riesgo han desempeñado en los procesos de toma de decisiones y los principales factores considerados en las decisiones que producen efectos jurídicos significativos o que impactan de manera considerable en la vida de las personas. Esto es fundamental para asegurar que cualquier persona afectada por tales decisiones entienda si estas pudiesen tener consecuencias adversas para su salud, seguridad o derechos fundamentales.

7.- Uso compatible de los sistemas de IA con el cumplimiento de la normativa de protección de datos de forma que las AAPP cumplirán con todas sus obligaciones en materia de protección de datos:

Las medidas siguientes deben ser contempladas en el marco de una **evaluación de impacto en la protección de datos (EIPD)** siguiendo lo establecido en el RGPD a través de la cual, además de identificar las amenazas para los derechos, en particular el derecho a la protección de datos y libertades fundamentales de las personas afectadas se evalúa el riesgo en las distintas fases del tratamiento, y en particular, el sesgo en los sistemas de toma de decisiones sobre las personas o su discriminación y las medidas para la mitigación del riesgo. En la primera fase de la EIPD las AAPP deben evaluar la **necesidad, idoneidad y proporcionalidad del uso del sistema de IA** con relación al objeto del tratamiento y si este puede o no alcanzarse mediante una solución alternativa y un menor nivel de riesgo para los derechos, en particular a la protección de datos, y libertades de las personas afectadas.

Las siguientes medidas de cumplimiento del RGPD se cumplirán y contemplarán como medidas de mitigación del riesgo y responsabilidad proactiva:

- **Persona del Delegado de Protección de Datos:** Las AAPP garantizarán en todo momento la participación de la persona Delegada de Protección de Datos, que ejercerá sus funciones de asesoramiento y supervisión sobre la IA con relación a su impacto con el tratamiento de datos personales.
- **Inventario y registro de actividad del tratamiento:** Exige a las AAPP identificar e inventariar los tratamientos de datos que se llevarán a cabo a través del sistema de IA y además hacer público el inventario de las actividades de tratamiento por medios electrónicos.
- **Principio de lealtad:** Exige a las AAPP hacer un uso de los datos que sea previsible por parte de las personas (en relación con la finalidad buscada) y que no haya consecuencias adversas para las personas que no estén justificadas.

- **Principio de exactitud:** Exige a las AAPP utilizar datos, ya sean directamente recogidos, inferidos o proporcionados por terceros, exactos, garantizando que el sistema de IA, en particular para la elaboración de perfiles” identifique y relacione a la persona afectada de forma exacta y con datos estables y predecibles. Las AAPP deben igualmente garantizar la superación del juicio de compatibilidad respecto del uso de datos obtenidos para un fin original y que posteriormente se someterán al sistema de IA con otro fin.
- **Principio de licitud:** Exige a las AAPP la recogida y tratamiento de datos personales de forma legítima.
- **Principio de minimización:** Exige a las AAPP tratar únicamente los datos que son estrictamente necesarios, así como el uso de técnicas que reducen la cantidad de datos necesarios (anonimización, generación de datos sintéticos, selección de atributos y aprendizaje federado), teniendo en cuenta, no obstante, que el efecto que una reducción de datos puede tener sobre la precisión del sistema y sobre la aparición de sesgos.
- **Principio de transparencia:** Exige a las AAPP informar del tratamiento de los datos personales bajo el sistema de IA y en particular de su derecho a conocer la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para las personas interesadas y, cuando corresponda, a obtener intervención humana por parte de la AAPP responsable, a que la persona interesada exprese su punto de vista y a impugnar la decisión adoptada.
- **Principio de limitación de la finalidad:** Exige a las AAPP acatar la norma de que los datos se recogerán para una finalidad específica y explícita, y que no se deben utilizar los datos de manera incompatible. Por tanto, las AAPP deben garantizar que el uso de los datos no es incompatible con la finalidad que motivó la recogida de datos. Este principio es esencial para que las personas puedan hacer un control efectivo del uso que se hace de sus datos.
- **Medidas de seguridad:** Acordes con lo establecido en el ENS.
- **Ejercicio de derechos:** Exige a las AAPP garantizar el ejercicio de los derechos de protección de datos, incluido el derecho de reclamación y denuncia ante las autoridades competentes, así como el derecho a no ser objeto de decisiones automatizadas derivadas de los sistemas de IA, y en su

caso, cuando corresponda, a obtener intervención humana por parte de la AAPP responsable, a que la persona interesada exprese su punto de vista y a impugnar la decisión adoptada.

- **Limitación del plazo de conservación y bloqueo de los datos:** Exige a las AAPP cesar en el tratamiento de los datos cuando estos dejan de ser necesarios para los fines que motivaron el mismo y concretamente el uso del sistema de IA, siendo relevante el bloqueo para atender un recurso o reclamación de las personas interesadas.

8.- Notificación del uso de los sistemas de IA de alto riesgo a la autoridad competente en el registro de conformidad: En los casos que corresponda y con carácter previo a poner en servicio o utilizar un sistema de IA de alto riesgo las AAPP se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE contemplada en la Ley de IA.

9.- Supervisión y control: Las AAPP deberán establecer medidas de control y supervisión constante del uso de los sistemas de IA y su conformidad de acuerdo con la normativa vigente y principios de este decálogo, incluidas auditorías, así como en particular, constante evaluación de la existencia de sesgos, corrigiendo defectos y aplicando mejoras y cambios legales y doctrinales derivados de las autoridades de control y supervisión.

10.- Responsabilidad por daños: las AAPP deberán asumir su responsabilidad en caso de fallo de los algoritmos de IA utilizados.