ESTUDIOS

LOS RETOS QUE PLANTEA LA INTELIGENCIA ARTIFICIAL A LA ADMINISTRACIÓN PÚBLICA

ALFONSO ORTEGA GIMÉNEZ
DIRECTOR
LERDYS SARAY HEREDIA SÁNCHEZ
COORDINADORA

UNIVERSITAS Miguel Hernández
DIPUTACIÓN DE ALICANTE
ARANZADI

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es

Atención al cliente: https://areacliente.aranzadilaley.es

Esta publicación se inserta dentro del Proyecto de Investigación 2024/con/00098. En el marco del convenio de la Excma. Diputación provincial de alicante con la Universidad Miguel Hernández de Elche y la Universidad de Alicante para impulsar los procesos de innovación, generación y transferencia de conocimientos y tecnología en el ámbito de la inteligencia digital_año 2024 (convocatoria de expresiones de interés 2024 de la Universidad Miguel Hernández de Elche de Proyectos de Investigación para impulsar los procesos de innovación, generación y transferencia de conocimientos y tecnología en el ámbito de la inteligencia digital (código línea 04-541-7-2024-0159-n)).

Primera edición: Junio 2025

Depósito Legal: M-14673-2025
ISBN versión impresa: 978-84-1085-198-6
ISBN versión electrónica: 978-84-1085-199-3

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

Índice General

19

Protocolo para la implantación de la inteligencia artificial en los servicios municipales de la provincia de Alicante, adaptado al nuevo reglamento europeo de inteligencia artificial[1]

Alfonso Ortega Giménez
Profesor Titular de Derecho internacional privado
de la Universidad Miguel Hernández
de Elche (Alicante)-Spain
ORCID: 0000-0002-8313-2070

Lerdys Saray Heredia Sánchez
Profª Derecho internacional privado
Universidad Miguel Hernández de Elche
ORCID: 0000-0003-1092-8868

SUMARIO: I. PLANTEAMIENTO. II. NORMATIVA APLICABLE. III. IMPLICACIONES EN PRIVACIDAD Y PROTECCIÓN DE DATOS. IV. CRITERIOS DE EVALUACIÓN DE RIESGOS PREVIO AL USO DE LA IA. V. SECTORES CLAVES DEL USO DE LA IA POR LA ADMINISTRACIÓN. VI. RÉGIMEN DE SANCIONES. VII. CONCLUSIONES.

1. El presente texto parte de la investigación llevada a cabo por el equipo del área de Derecho internacional privado y se nutre de los estudios realizados por el Dr. D. Alfonso Ortega Giménez sobre el impacto del Reglamento Europeo de IA.

I. PLANTEAMIENTO

Desde una perspectiva amplia puede definirse como sistema de IA como cualquier programa informático que utiliza técnicas automatizadas para procesar datos y generar resultados que, tradicionalmente, habrían requerido intervención humana. Este concepto abarca tanto los sistemas que operan de manera autónoma como aquellos diseñados para complementar las capacidades humanas.

La Inteligencia Artificial (IA) puede ser definida como «*la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparable s a la que realiza la mente humana, como el aprendizaje o el razonamiento lógico*».

La distinción entre sistemas integrados e independientes es crucial porque determina las responsabilidades de los desarrolladores y operadores, así como las normativas específicas que se aplican a cada tipo de sistema. Mientras que los sistemas integrados deben garantizar una interacción segura y efectiva con el hardware en el que están incorporados, los sistemas independientes deben centrarse en la protección de datos, la transparencia de las decisiones y la accesibilidad del usuario.

Esta diferenciación también refleja cómo la IA puede adaptarse a una variedad de contextos, desde aplicaciones físicas hasta entornos digitales, lo que subraya su versatilidad y potencial transformador.

Con la IA como elemento central, el presente documento pone a disposición de la Administración Local los elementos claves a tener en cuenta para que su uso se ajuste a los requerimientos legales en aquellas áreas donde las herramientas digitales se introducen.

II. NORMATIVA APLICABLE

La creciente preocupación por los riesgos asociados con la IA también ha sido un motor importante para el desarrollo de la norma. Las implicaciones éticas, sociales y legales de la IA han generado debates intensos sobre temas como la transparencia, la responsabilidad y la equidad. Por ejemplo, la opacidad de los algoritmos de aprendizaje automático, a menudo descritos como «cajas negras», plantea desafíos para comprender cómo se toman las decisiones y cómo pueden ser supervisadas o auditadas.

Esto se complica aún más cuando estas decisiones tienen un impacto significativo en la vida de las personas, como en los casos de contratación,

asignación de recursos o evaluaciones de crédito. Además, los sesgos inherentes en los datos utilizados para entrenar sistemas de IA pueden perpetuar desigualdades y discriminaciones, lo que subraya la necesidad de garantizar que estas tecnologías sean justas y representativas. Estos riesgos, junto con las preocupaciones sobre la vigilancia masiva, la manipulación de la opinión pública y el uso indebido de la IA en conflictos armados, han impulsado la urgencia de establecer un marco normativo que aborde de manera integral las posibles. La normativa europea de aplicación es 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.º 300/2008 (UE) n.º 167/2013 (UE) n.º 168/2013 (UE) 2018/858 (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE (UE) 2016/797 y (UE) 2020/1828 (*Reglamento de Inteligencia Artificial*)[2].

1. Objetivos del Reglamento europeo de IA.

– Garantizar el desarrollo y la utilización de sistemas de IA confiables, éticos y centrados en el ser humano. La UE busca asegurar que la IA no solo sea tecnológicamente avanzada, sino también alineada con los valores fundamentales de la Unión, como el respeto a la dignidad humana, la democracia, el Estado de derecho y la protección de los derechos fundamentales. Para ello, el Reglamento establece normas claras que promueven una IA que beneficie a la sociedad en su conjunto, evitando usos perjudiciales o discriminatorios. Este enfoque se fundamenta en el principio de que la tecnología debe servir a las personas, mejorando su calidad de vida sin comprometer su autonomía ni su seguridad.

– Prevenir y mitigar los riesgos asociados con los sistemas de IA, especialmente aquellos que pueden tener un impacto significativo en la salud, la seguridad y los derechos de los ciudadanos. El Reglamento introduce un enfoque basado en riesgos, que clasifica los sistemas de IA en diferentes categorías según su nivel de riesgo.

– Promoción de la transparencia en los sistemas de IA es otro objetivo clave del Reglamento. La opacidad de algunos algoritmos y la falta de explicabilidad de sus decisiones han generado preocupación tanto entre los legisladores, como entre los ciudadanos. El Reglamento exige que los sistemas de IA proporcionen información

2. DOUE núm. 1689, de 12 de julio de 2024.

clara sobre su funcionamiento, limitaciones y objetivos. Esto incluye garantizar que los usuarios estén debidamente informados cuando interactúan con un sistema de IA, especialmente en contextos en los que puede influir en decisiones que les afecten significativamente, como evaluaciones crediticias, procesos de selección de personal o diagnósticos médicos. Al fomentar la transparencia, la UE busca aumentar la confianza del público en estas tecnologías y garantizar que los usuarios puedan tomar decisiones informadas al interactuar con ellas.

– La protección de los derechos fundamentales de los ciudadanos europeos frente a posibles abusos o impactos negativos de la IA. Entre los derechos protegidos se incluyen el derecho a la privacidad, la no discriminación, la seguridad personal y la libertad de elección. Por ejemplo, se prohíben prácticas como la puntuación social, la manipulación psicológica y el uso indiscriminado de tecnologías de reconocimiento facial en espacios públicos. Estas restricciones reflejan el compromiso de la UE de evitar aplicaciones de la IA que puedan socavar los principios democráticos, fomentar desigualdades o generar dinámicas de vigilancia masiva. Además, el Reglamento refuerza la protección de los datos personales, asegurando que cualquier tratamiento de datos en sistemas de IA cumpla con las estrictas normativas ya existentes en la UE, como el RGPD.

– Fomentar la innovación y el desarrollo tecnológico dentro de la UE, promoviendo un entorno que permita a las empresas europeas competir a nivel global. La UE reconoce la importancia de la IA como motor de crecimiento económico y transformación digital, y busca garantizar que las empresas, incluidas las pequeñas y medianas empresas (PYMEs), tengan acceso a recursos y herramientas para desarrollar y desplegar sistemas de IA de manera segura y eficiente. Para ello, el Reglamento introduce medidas específicas destinadas a apoyar a las PYMEs, como la simplificación de los procedimientos regulatorios y la creación de espacios controlados de pruebas, conocidos como sandbox, que permiten experimentar con tecnologías de IA en entornos controlados sin estar sujetas a todas las restricciones normativas.

El Reglamento establece un marco claro para la supervisión y el control de las acciones ejecutadas mediante IA y la creciente preocupación por los riesgos asociados con la IA también ha sido un motor importante para el

desarrollo de la norma. Las implicaciones éticas, sociales y legales de la IA han generado debates intensos sobre temas como la transparencia, la responsabilidad y la equidad. Por ejemplo, la opacidad de los algoritmos de aprendizaje automático, a menudo descritos como «cajas negras», plantea desafíos para comprender cómo se toman las decisiones y cómo pueden ser supervisadas o auditadas.

Los principios legales son pieza clave cuando estas decisiones tienen un impacto significativo en la vida de las personas, como en los casos de contratación, asignación de recursos o evaluaciones de crédito. Además, los sesgos inherentes en los datos utilizados para entrenar sistemas de IA pueden perpetuar desigualdades y discriminaciones, lo que subraya la necesidad de garantizar que estas tecnologías sean justas y representativas. Estos riesgos, junto con las preocupaciones sobre la vigilancia masiva, la manipulación de la opinión pública y el uso indebido de la IA en conflictos armados, han impulsado la urgencia de establecer un marco normativo que aborde de manera integral las posibles

El Reglamento establece un marco claro para la supervisión y el control de las acciones ejecutadas mediante IA y su estructura es la siguiente:

Título o Sección	Contenido	Objetivo
Disposiciones Generales	Definición de términos clave, ámbito de aplicación, principios éticos y objetivos del Reglamento.	Establecer un marco legal uniforme y claro para regular el desarrollo y uso de sistemas de IA.
Clasificación de Sistemas	Jerarquía de riesgos: sistemas de riesgo inaceptable, alto, limitado y mínimo, con ejemplos para cada categoría.	Garantizar que la regulación sea proporcional al impacto y riesgo asociado de los sistemas de IA.
Requisitos para Sistemas de Alto Riesgo	Obligaciones técnicas, éticas y operativas para sistemas que impactan significativamente en la seguridad y derechos fundamentales.	Proteger a los usuarios garantizando seguridad, transparencia y supervisión.
Prácticas Prohibidas	Lista de aplicaciones de IA incompatibles con los principios éticos de la UE, como manipulación subliminal y puntuación social.	Salvaguardar derechos fundamentales y evitar abusos de las tecnologías de IA.

Título o Sección	Contenido	Objetivo
Obligaciones de Proveedores y Operadores	Responsabilidades específicas en diseño, implementación, documentación, gestión de datos y monitoreo post-comercialización.	Asegurar el cumplimiento normativo y la supervisión a lo largo del ciclo de vida del sistema de IA.
Espacios de Pruebas Regulados (Sandboxes)	Entornos controlados para la experimentación de tecnologías innovadoras bajo supervisión regulatoria.	Fomentar la innovación responsable y apoyar a startups y PYMEs.
Transparencia y Trazabilidad	Requisitos para explicar el funcionamiento de los sistemas, registrar decisiones y documentar fuentes de datos.	Garantizar la rendición de cuentas y fortalecer la confianza pública en la IA.
Gobernanza y Supervisión	Rol de las autoridades nacionales, el Comité Europeo de IA y mecanismos de supervisión del mercado.	Coordinar la implementación del Reglamento y garantizar la conformidad en toda la UE.
Sanciones y Cumplimiento	Régimen de sanciones por incumplimiento, diferenciando entre infracciones leves, graves y muy graves.	Disuadir prácticas ilegales y fomentar el cumplimiento normativo.
Medidas de Apoyo a la Innovación	Códigos de conducta voluntarios, incentivos financieros y promoción de buenas prácticas en el desarrollo de IA.	Facilitar el desarrollo de tecnologías seguras y responsables.

III. IMPLICACIONES EN PRIVACIDAD Y PROTECCIÓN DE DATOS

Las implicaciones en privacidad y protección de datos derivadas del uso de la IA son vastas y complejas, abarcando una amplia gama de preocupaciones relacionadas con la recopilación, el almacenamiento, el procesamiento y el uso de datos personales. En un mundo donde la IA desempeña un papel creciente en la vida cotidiana, desde servicios digitales personalizados hasta sistemas de vigilancia avanzada y herramientas automatizadas de toma de decisiones, el manejo de datos se ha convertido en un tema central para garantizar que estas tecnologías respeten los derechos fundamentales de las personas.

La privacidad no solo es un derecho intrínseco protegido por leyes y normativas como el RGPD en Europa, sino que también constituye un pilar esencial para construir la confianza del público en las tecnologías basadas en IA. La manera en que se gestionan los datos puede influir directamente en la aceptación y el éxito de estas tecnologías, determinando si se perciben como herramientas beneficiosas o invasivas.

Uno de los aspectos más significativos de las implicaciones en privacidad y protección de datos en la IA es la magnitud de la recopilación de información personal. Los sistemas de IA, especialmente aquellos que emplean aprendizaje automático, dependen de grandes volúmenes de datos para entrenar sus algoritmos y mejorar su precisión y funcionalidad. Estos datos pueden incluir información personal altamente sensible, como nombres, direcciones, registros médicos, datos financieros, hábitos de consumo y comportamientos en línea. En algunos casos, los sistemas de IA también procesan datos biométricos, como huellas dactilares, reconocimiento facial y patrones de voz, lo que aumenta las preocupaciones debido a la naturaleza única y permanente de estos datos. La recopilación masiva y el uso intensivo de datos presentan un riesgo inherente, ya que cualquier mal manejo puede exponer a las personas a violaciones de privacidad, discriminación, manipulación o incluso daño físico.

La naturaleza de los algoritmos de IA también plantea desafíos únicos para la privacidad. En muchos casos, los sistemas de IA pueden analizar y correlacionar datos aparentemente inofensivos para extraer información sensible o predecir comportamientos futuros, a menudo sin que las personas sean conscientes de la profundidad de este análisis. Por ejemplo, un sistema diseñado para analizar patrones de compra podría inferir detalles sobre la salud, las creencias religiosas o las preferencias políticas de un individuo[3]. La capacidad de la IA para procesar y analizar datos de manera tan poderosa exige salvaguardias estrictas para garantizar que el uso de estos datos sea ético y transparente.

Otro aspecto crucial relacionado con la privacidad y la protección de datos es la falta de control que los individuos a menudo experimentan sobre su información personal. En muchos casos, los datos son recopilados sin el conocimiento explícito de los usuarios o sin un consentimiento informado

3. Este tipo de inferencias puede ser particularmente problemático cuando los datos son utilizados para tomar decisiones automatizadas que afectan directamente a las personas, como la aprobación de créditos, la contratación laboral o la asignación de recursos públicos.

claro, lo que socava su capacidad para decidir cómo se utiliza su información. Incluso cuando las personas dan su consentimiento, este suele estar limitado por la falta de comprensión de los términos y condiciones, o por la incapacidad de prever todas las formas en que sus datos podrían ser utilizados en el futuro. Esta falta de control no solo genera preocupaciones éticas, sino que también puede erosionar la confianza en las empresas y organizaciones que desarrollan y operan sistemas de IA, afectando su reputación y su capacidad para generar aceptación pública.

La seguridad de los datos es otra dimensión crítica de las implicaciones en privacidad asociadas con la IA. La recopilación y el almacenamiento de grandes volúmenes de datos personales crean objetivos atractivos para los ciberdelincuentes, aumentando el riesgo de violaciones de datos que pueden tener consecuencias devastadoras para las personas afectadas. Además, los sistemas de IA en sí mismos pueden ser vulnerables a ataques, como el envenenamiento de datos, que buscan manipular los algoritmos mediante la introducción de datos maliciosos[4].

La transparencia es otro aspecto fundamental para abordar las implicaciones en privacidad y protección de datos en la IA. Muchas personas desconocen cómo se recopilan, procesan y utilizan sus datos, lo que genera una desconexión entre los usuarios y las organizaciones responsables de los sistemas de IA. Para mitigar este problema, es crucial que los desarrolladores y operadores de IA proporcionen información clara y accesible sobre sus prácticas de manejo de datos, incluida la finalidad de la recopilación, el tipo de datos recopilados, las fuentes de los datos y cómo se comparten o se venden a terceros. La transparencia no solo permite a las personas tomar decisiones informadas sobre el uso de sus datos, sino que también facilita la supervisión por parte de las autoridades reguladoras y la sociedad civil, promoviendo una mayor rendición de cuentas.

El diseño ético y responsable de los sistemas de IA también es esencial para abordar las implicaciones en privacidad y protección de datos. Esto incluye la adopción de enfoques como la privacidad desde el diseño y la privacidad por defecto, que integran principios de protección de datos

4. Estas amenazas subrayan la importancia de implementar medidas de seguridad robustas, como la encriptación de datos, la detección de intrusiones y la autenticación multifactorial, para proteger la información personal frente a accesos no autorizados. Sin embargo, garantizar la seguridad de los datos no es suficiente si no se acompaña de prácticas responsables de recopilación y uso, ya que incluso los datos más protegidos pueden ser utilizados de manera indebida si los sistemas de IA no están diseñados y gestionados con principios éticos en mente.

en todas las etapas del ciclo de vida del sistema, desde la recopilación inicial de datos hasta su procesamiento, almacenamiento y eliminación. Estas prácticas garantizan que los sistemas de IA minimicen el uso de datos personales, procesen solo la información estrictamente necesaria para cumplir con su propósito y eviten el uso excesivo o inapropiado de los datos. Además, el diseño ético también implica garantizar que los sistemas de IA sean explicables y auditables, permitiendo a los usuarios y reguladores comprender y evaluar cómo se toman las decisiones basadas en datos.

Las implicaciones en privacidad y protección de datos también tienen un impacto significativo en la equidad y la inclusión. En muchos casos, las prácticas de recopilación de datos pueden reflejar y perpetuar desigualdades existentes, excluyendo a ciertos grupos de población o tratándolos de manera desproporcionada. Por ejemplo, los sistemas de IA entrenados con datos sesgados pueden discriminar a individuos en función de su raza, género, orientación sexual o nivel socioeconómico, lo que puede resultar en decisiones injustas o incluso ilegales[5].

Las implicaciones en privacidad y protección de datos en la IA son un desafío complejo pero esencial que requiere un enfoque integral y basado en principios. Al adoptar medidas como la transparencia, la seguridad, el diseño ético y la colaboración internacional, se puede garantizar que las tecnologías de IA respeten los derechos fundamentales de las personas y promuevan el bienestar social. Este enfoque no sólo protege a los usuarios y fortalece la confianza en la IA, sino que también sienta las bases para un ecosistema de innovación responsable y sostenible, que maximice los beneficios de estas tecnologías al tiempo que minimice sus riesgos e impactos negativos.

La privacidad y la protección de datos no son solo consideraciones técnicas o legales, sino valores fundamentales que deben estar en el centro de cualquier esfuerzo para desarrollar y utilizar la IA de manera ética y responsable.

5. Para abordar estos problemas, es fundamental que los desarrolladores y operadores de IA adopten un enfoque inclusivo y diverso en la recopilación y el manejo de datos, garantizando que los conjuntos de datos sean representativos y libres de sesgos. Además, las organizaciones deben realizar auditorías regulares para identificar y corregir posibles desigualdades en el tratamiento de los datos y en los resultados generados por los sistemas de IA.

IV. CRITERIOS DE EVALUACIÓN DE RIESGOS PREVIO AL USO DE LA IA

¿Es necesario usar IA para determinada tarea? ¿Existen alternativas convencionales? ¿Es apropiado el uso de IA? ¿Hay restricciones específicas? Riesgo ¿Cuál es el nivel de sensibilidad? ¿Qué impacto podría tener un error en su uso por parte de la Administración?

El enfoque de categorización basado en riesgos permite clasificar los sistemas de IA en función del impacto que tienen en la seguridad, los derechos fundamentales y el bienestar de las personas, estableciendo un conjunto de obligaciones y restricciones adaptadas al nivel de riesgo asociado.

Este enfoque tiene como objetivo equilibrar la promoción de la innovación tecnológica con la necesidad de salvaguardar valores esenciales de la UE, como la dignidad humana, la privacidad, la equidad y la democracia.

Categorías de riesgos:

– **riesgo inaceptable**: La categoría de riesgo inaceptable en el ámbito de la IA representa un compromiso firme de la UE con la protección de los derechos fundamentales y la preservación de los valores éticos que sustentan su marco normativo y social. Estas tecnologías, por su naturaleza intrínseca, son consideradas incompatibles con principios fundamentales como la dignidad humana, la libertad individual y la privacidad, lo que ha llevado a su prohibición estricta dentro del territorio de la Unión. Este enfoque no solo establece límites claros para el desarrollo y uso de sistemas de IA, sino que también envía un mensaje inequívoco sobre la importancia de priorizar la seguridad, la equidad y el respeto por los derechos en el diseño y la implementación de estas tecnologías avanzadas.

Una de las aplicaciones prohibidas bajo esta categoría es la manipulación subliminal, una práctica que plantea amenazas significativas a la autonomía personal y la toma de decisiones informada. Estos sistemas de IA están diseñados para influir en las decisiones humanas mediante estímulos subliminales, lo que significa que los individuos no son conscientes de la intervención tecnológica en su proceso de razonamiento o comportamiento[6].

6. Un ejemplo de esto podría ser una aplicación de marketing que utiliza algoritmos de IA para enviar mensajes subliminales dirigidos a persuadir a los usuarios de adquirir productos específicos.

Esta forma de manipulación no solo socava la capacidad de las personas para tomar decisiones libres e informadas, sino que también plantea cuestiones éticas sobre el consentimiento y la explotación de vulnerabilidades cognitivas. Al prohibir estas tecnologías, la UE refuerza su compromiso de proteger la autonomía y la libertad de sus ciudadanos, asegurando que las interacciones con los sistemas de IA sean transparentes y respetuosas de la dignidad humana.

Otra tecnología incluida en la categoría de riesgo inaceptable es la puntuación social, un sistema inspirado en prácticas observadas en otros contextos, como el modelo implementado en China. La puntuación social implica evaluar y clasificar a las personas en función de su comportamiento, actividades o interacciones sociales, generando perfiles que pueden ser utilizados para otorgar o restringir derechos, beneficios o acceso a servicios. Aunque este tipo de sistema se presenta como una herramienta para fomentar comportamientos positivos, plantea riesgos graves de discriminación, exclusión social y concentración de poder en manos de quienes gestionan estas plataformas. La posibilidad de que autoridades o empresas privadas utilicen la puntuación social para influir en la vida de las personas de manera desproporcionada o arbitraria genera una dinámica de control que es incompatible con los valores democráticos y los derechos fundamentales que defiende la UE. La prohibición de estos sistemas refuerza la necesidad de garantizar que las tecnologías de IA no se utilicen para socavar la igualdad de oportunidades, la justicia social y la libertad individual.

El Reglamento también prohíbe el uso de tecnologías de vigilancia biométrica masiva en espacios públicos, una práctica que plantea serias preocupaciones sobre la privacidad, la libertad y el potencial abuso estatal. Estas tecnologías, que incluyen herramientas como el reconocimiento facial y otros sistemas biométricos, permiten una monitorización indiscriminada de las personas en lugares públicos, recopilando y analizando datos biométricos sensibles sin el consentimiento de los individuos afectados. Esta forma de vigilancia masiva no solo representa una intrusión significativa en la privacidad personal, sino que también genera un entorno de control y vigilancia que puede tener un efecto disuasorio en el ejercicio de libertades fundamentales como la libertad de expresión, reunión y movimiento.

La inclusión de estas tecnologías en la categoría de riesgo inaceptable no es solo una respuesta a los riesgos inmediatos que plantean, sino también una medida preventiva frente a posibles futuros abusos y desarrollos no deseados.

– **alto riesgo:** Los sistemas de IA clasificados como de alto riesgo buscan equilibrar la innovación tecnológica con la protección de los

> derechos fundamentales, la seguridad y el bienestar de las personas. Estas aplicaciones se implementan en sectores críticos donde su impacto puede ser profundo, afectando decisiones y situaciones que tienen consecuencias directas para los individuos y la sociedad en su conjunto. En el ámbito de la sanidad, los sistemas de IA han demostrado un potencial transformador al mejorar los diagnósticos y optimizar los tratamientos médicos. Herramientas que analizan imágenes médicas como radiografías y tomografías para detectar anomalías son un claro ejemplo de cómo la IA puede ofrecer resultados más rápidos y precisos que los métodos tradicionales.

En el ámbito de la infraestructura crítica y el transporte, la IA está transformando la manera en que operan los sistemas fundamentales para la sociedad. Los vehículos autónomos, por ejemplo, dependen de la IA para la navegación y el control del vehículo, lo que promete reducir accidentes causados por errores humanos y aumentar la eficiencia en el transporte. Asimismo, los sistemas de gestión de redes eléctricas y otras infraestructuras críticas utilizan algoritmos avanzados para optimizar la distribución de recursos, mejorar la sostenibilidad y prevenir interrupciones. Sin embargo, estos sistemas también presentan riesgos inherentes, ya que cualquier fallo en los algoritmos o en su implementación puede tener consecuencias catastróficas para la seguridad y el funcionamiento de los servicios esenciales. La evaluación de conformidad previa, la supervisión humana constante y la documentación detallada son imprescindibles para minimizar estos riesgos y garantizar la fiabilidad de estas aplicaciones.

El Reglamento establece una serie de requisitos para los sistemas de IA clasificados como de alto riesgo, diseñados para garantizar su seguridad, equidad y responsabilidad. Antes de que estos sistemas puedan ser comercializados o implementados, deben someterse a evaluaciones exhaustivas que incluyan *auditorías técnicas, pruebas de seguridad y validaciones algorítmicas p*ara verificar su cumplimiento con los estándares normativos. Además, los operadores humanos deben estar capacitados para intervenir y anular las decisiones automatizadas en situaciones críticas, asegurando que siempre exista un nivel de control humano sobre los sistemas.

La trazabilidad y la documentación también son fundamentales, ya que permiten mantener registros detallados sobre el funcionamiento de los sistemas, las fuentes de datos utilizadas y los procesos de toma de decisiones, lo que facilita las auditorías y la identificación de fallos. Los desarrolladores también están obligados a implementar estrategias de gestión de riesgos que

incluyan la identificación, evaluación y mitigación de posibles problemas durante todo el ciclo de vida del sistema.

Requisitos Clave para Sistemas de Alto Riesgo.

Categoría de Requisitos	Descripción	Ejemplos de Implementación
Gestión de Riesgos	Los proveedores deben identificar, evaluar y mitigar los riesgos potenciales en todo el ciclo de vida del sistema.	– Análisis de impacto inicial – Evaluaciones periódicas de seguridad y desempeño
Gobernanza de Datos	Garantizar que los datos utilizados sean representativos, de alta calidad y estén libres de sesgos para decisiones justas.	– Procedimientos de limpieza de datos – Documentación detallada de las fuentes de datos
Transparencia	Proporcionar información clara sobre cómo funciona el sistema, sus limitaciones y los criterios utilizados en sus decisiones.	– Manuales de usuario explicativos – Descripciones accesibles para usuarios y operadores
Supervisión Humana	Asegurar que los sistemas permitan la intervención humana cuando sea necesario, especialmente en decisiones críticas.	– Interfaces para anular decisiones automatizadas – Capacitación a operadores para supervisión efectiva
Ciberseguridad	Proteger los sistemas contra ataques cibernéticos y garantizar su funcionamiento seguro bajo condiciones adversas.	– Implementación de medidas de encriptación – Actualizaciones de seguridad periódicas
Documentación Técnica	Mantener un registro exhaustivo sobre el diseño, los algoritmos utilizados, los datos de entrenamiento y los resultados de pruebas.	– Informes técnicos detallados disponibles para auditorías y autoridades regulatorias
Monitoreo Post-Comercialización	Establecer mecanismos para recopilar datos sobre el uso del sistema, identificar fallos y notificar incidentes relevantes.	– Sistemas automáticos de registro de errores – Informes de uso enviados a las autoridades competentes
Evaluación de Conformidad	Realizar auditorías y pruebas para verificar que el sistema cumple con los estándares técnicos, legales y éticos establecidos.	– Auditorías internas y externas – Certificaciones emitidas por organismos autorizados

Fuente: elaboración propia, a partir del Reglamento europeo de IA.

- **riesgo limitado:** Los sistemas de IA clasificados como de riesgo limitado no presentan un impacto significativo en los derechos fundamentales o la seguridad, pero aún requieren ciertas garantías para mantener la transparencia y la confianza del usuario. Aplicaciones como asistentes virtuales y chatbots utilizados en atención al cliente son ejemplos comunes de esta categoría. Aunque estas herramientas son ampliamente utilizadas y no suelen plantear riesgos graves, es importante garantizar que los usuarios sean conscientes de que están interactuando con un sistema automatizado y no con un humano. Además, los operadores deben proporcionar explicaciones claras sobre cómo funcionan estos sistemas, cómo se toman las decisiones automatizadas y qué datos se utilizan. Este enfoque promueve la confianza pública y asegura que las interacciones con estas tecnologías sean transparentes y éticas,
- **riesgo mínimo:** son aquellos que tienen un impacto insignificante en los derechos fundamentales y la seguridad. Estas tecnologías, como los filtros de correo no deseado, los motores de búsqueda y las herramientas de edición de imágenes, son omnipresentes en la vida cotidiana y se consideran esencialmente inofensivas. El Reglamento permite que estos sistemas operen sin requisitos regulatorios específicos, lo que fomenta la innovación y reduce las barreras para su desarrollo y adopción. Este enfoque diferenciado refleja el principio de proporcionalidad, que adapta las obligaciones normativas al nivel de riesgo asociado con cada tipo de sistema de IA. Al mismo tiempo, el Reglamento busca garantizar que las aplicaciones más críticas estén sujetas a una supervisión estricta, minimizando los posibles daños para los ciudadanos y promoviendo la protección de los derechos fundamentales.

Esta clasificación permite aplicar normativas proporcionadas según las posibles consecuencias negativas de cada tipo de sistema, optimizando los recursos regulatorios y asegurando una supervisión más rigurosa en los casos en los que los daños potenciales sean mayores.

Nivel de Riesgo	Descripción	Ejemplos de Sistemas	Obligaciones/ Requisitos
Riesgo Inaceptable	Sistemas de IA cuyo uso está prohibido debido a su incompatibilidad con los derechos fundamentales y principios éticos.	– Manipulación subliminal – Puntuación social – Vigilancia biométrica masiva (con excepciones estrictas)	Prohibición total, salvo excepciones limitadas y reguladas (como casos de seguridad pública o prevención de delitos graves).

Nivel de Riesgo	Descripción	Ejemplos de Sistemas	Obligaciones/ Requisitos
Alto Riesgo	Sistemas de IA que impactan significativamente en derechos fundamentales, seguridad o bienestar de las personas, utilizados en sectores críticos.	– Diagnóstico médico – Evaluación crediticia – Selección de personal – Vehículos autónomos	– Evaluaciones rigurosas – Supervisión humana – Documentación exhaustiva – Registro en bases de datos.
Riesgo Limitado	Sistemas que no afectan de manera significativa a derechos fundamentales, pero que aún requieren ciertas garantías para garantizar la transparencia.	– Chatbots – Sistemas de recomendación (plataformas de streaming o comercio electrónico)	– Información clara al usuario sobre la interacción con IA – Explicabilidad básica de las decisiones.
Riesgo Mínimo	Tecnologías de IA consideradas esencialmente inofensivas y de bajo impacto.	– Filtros de correo no deseado – Motores de búsqueda – Edición de imágenes	Sin requisitos específicos bajo el Reglamento.

Los responsables del despliegue son las entidades que implementan y utilizan los sistemas de IA en sus operaciones diarias. Este grupo incluye empresas, organizaciones gubernamentales y otras entidades que integran la IA en sus procesos internos o en la prestación de servicios a los ciudadanos[7].

7. Además, el mantenimiento regular incluye la incorporación de mejoras y actualizaciones que puedan aumentar la eficiencia, la seguridad y la equidad del sistema, asegurando que este siga cumpliendo con los estándares más altos a lo largo de su ciclo de vida. Los responsables del despliegue de sistemas de IA abarcan una amplia variedad de sectores que integran estas tecnologías en sus operaciones para mejorar su eficiencia y efectividad. En el ámbito sanitario, los hospitales y centros médicos destacan como usuarios clave de la IA, empleándola para tareas como el diagnóstico de enfermedades, la gestión eficiente de recursos hospitalarios y la planificación de tratamientos personalizados. Por otro lado, las empresas de logística y transporte recurren a sistemas de IA para optimizar rutas de entrega, gestionar inventarios con mayor precisión y aumentar la eficiencia operativa en sus cadenas de suministro. Además, las entidades gubernamentales representan otro ejemplo destacado, utilizando la IA para mejorar la prestación de servicios públicos, facilitar la gestión de trámites administrativos y asignar recursos de manera más equitativa y eficiente. Estas organizaciones ilustran cómo la IA puede aplicarse en una variedad de contextos para transformar procesos clave y beneficiar tanto a las instituciones como a los usuarios finales.

1. **Implementación Ética y Responsable:** Los responsables del despliegue deben asegurarse de que los sistemas de IA se utilicen de manera compatible con los derechos fundamentales y los principios éticos. Esto incluye evitar el uso indebido de la tecnología y garantizar que las decisiones automatizadas no sean discriminatorias.

2. **Capacitación del Personal:** Es fundamental que los empleados que interactúan con los sistemas de IA reciban formación adecuada para comprender cómo funcionan, cómo interpretar sus resultados y cómo intervenir en caso de anomalías.

3. **Supervisión Continua:** Los responsables del despliegue deben monitorizar el desempeño de los sistemas de IA de manera continua, identificando posibles errores o riesgos y tomando medidas correctivas cuando sea necesario.

4. **Registro y Documentación:** Durante la operación de los sistemas, los responsables del despliegue están obligados a mantener registros detallados de las decisiones automatizadas y los resultados obtenidos. Esto facilita la rendición de cuentas y la resolución de disputas.

5. **Transparencia hacia los Usuarios:** Los responsables del despliegue deben informar a los usuarios finales cuando están interactuando con un sistema de IA, explicando claramente cómo funciona y cuáles son sus limitaciones.

Los **usuarios** son las personas o entidades que interactúan directamente con los sistemas de IA o que se ven afectadas por sus decisiones. Este grupo incluye tanto a consumidores individuales como a profesionales que utilizan la IA en su trabajo diario.

Los usuarios de sistemas de IA tienen derechos fundamentales y responsabilidades clave para garantizar un uso ético y seguro de estas tecnologías, entre los derechos más importantes se encuentran:

– El derecho a la transparencia, que asegura que los usuarios sean informados de manera clara cuando interactúan con un sistema de IA y reciban explicaciones comprensibles sobre su funcionamiento y las decisiones automatizadas que genera[8].

8. Además, cuando una decisión automatizada tiene un impacto significativo en la vida del usuario, este tiene el derecho de solicitar una revisión humana de dicha decisión, lo que refuerza la supervisión y la justicia en los procesos basados en IA.

– Los usuarios, especialmente aquellos que son profesionales en sectores como la medicina, el derecho o la educación, tienen la obligación de utilizar estos sistemas de manera ética y responsable, garantizando que las decisiones tomadas con el apoyo de la IA no vulneren derechos fundamentales ni perpetúen prácticas discriminatorias[9].

– Los usuarios de sistemas de IA abarcan una amplia gama de perfiles, desde consumidores individuales hasta profesionales y entidades gubernamentales, cada uno con necesidades y desafíos específicos al interactuar con estas tecnologías. Los consumidores individuales representan uno de los grupos más numerosos, utilizando asistentes virtuales como *Alexa o Siri,* interactuando con *chatbots* en servicios de atención al cliente o beneficiándose de recomendaciones personalizadas en plataformas digitales como servicios de *streaming* o comercio electrónico[10].

Los proveedores tienen la responsabilidad de ofrecer a los responsables del despliegue toda la información necesaria para que estos puedan implementar los sistemas de manera segura y conforme a la normativa. Esto incluye la entrega de documentación técnica detallada, la provisión de formación especializada para el personal encargado y el soporte continuo para resolver cualquier problema que pueda surgir durante la operación del sistema.

La transparencia también implica que los usuarios sean claramente informados cuando están interactuando con un sistema de IA, lo que incluye detalles sobre la naturaleza del sistema, como si es un *chatbot* o un motor de recomendación, y los objetivos que persigue, así como su posible influencia en las decisiones del usuario. Finalmente, la trazabilidad es un componente clave de la transparencia, ya que los sistemas deben registrar y documentar todas las decisiones tomadas, así como los datos y algoritmos utilizados. Esto permite que los sistemas sean auditados y revisados en caso de errores o disputas, asegurando la rendición de cuentas y facilitando la resolución de

9. Para ello, es esencial que los usuarios profesionales reciban una formación adecuada que les permita comprender a fondo cómo funcionan los sistemas, interpretar sus resultados y utilizarlos de manera efectiva en su trabajo cotidiano, asegurando siempre un enfoque basado en la responsabilidad y la protección de los derechos de todas las personas involucradas.

10. Las entidades gubernamentales también son usuarios clave, aprovechando los sistemas de IA para mejorar la prestación de servicios públicos, gestionar grandes volúmenes de datos y tomar decisiones más informadas en áreas como la asignación de recursos o la evaluación de políticas.

problemas. Este enfoque integral de la transparencia fomenta la confianza en la IA y asegura que su uso sea ético y responsable.

Los requisitos de protección de datos y privacidad en los sistemas de IA, según el Reglamento europeo de IA, están alineados con el cumplimiento estricto del RGPD. Esto exige que todos los sistemas procesen los datos personales de manera lícita, justa y transparente, asegurando que estén protegidos frente a accesos no autorizados, pérdidas o manipulaciones[11].

Los requisitos del Reglamento europeo de IA establecen principios claros para garantizar la supervisión humana, la equidad, la robustez, la precisión, y la adecuada documentación y registro de los sistemas de IA:

- En cuanto a la supervisión humana, los sistemas deben estar diseñados para permitir la intervención humana en cualquier momento, especialmente en situaciones críticas. Esto implica que los operadores puedan anular decisiones automatizadas cuando sea necesario y que los sistemas no actúen de manera completamente autónoma en contextos de alto riesgo. Además, es fundamental que los operadores humanos reciban formación adecuada para comprender el funcionamiento del sistema, interpretar sus resultados y tomar decisiones informadas en base a estos.

- En lo que respecta a la equidad y la no discriminación, los desarrolladores están obligados a identificar y eliminar posibles sesgos en los datos utilizados para entrenar los sistemas de IA, lo que incluye analizar las fuentes de datos para garantizar que sean representativas y equilibradas. Asimismo, los sistemas de IA deben someterse a evaluaciones periódicas para asegurar que no generen resultados discriminatorios o desiguales para diferentes grupos de personas. También se deben establecer mecanismos que permitan a los usuarios afectados por decisiones automatizadas solicitar una revisión humana, fortaleciendo la confianza en estas tecnologías.

11. Además, los sistemas deben adherirse al principio de minimización de datos, lo que significa que solo se deben recopilar y procesar los datos estrictamente necesarios para cumplir con el propósito específico del sistema, evitando el uso excesivo o no autorizado de información personal. Por otra parte, cuando sea necesario, se requiere el consentimiento explícito de los usuarios antes de procesar sus datos personales. Este consentimiento debe basarse en una comunicación clara que informe al usuario sobre cómo se utilizarán sus datos, permitiéndole tomar decisiones informadas. Estas medidas garantizan que los derechos de privacidad de los individuos estén protegidos y que los sistemas de IA operen de manera ética y conforme a la normativa europea.

– En términos de robustez y precisión, los sistemas de IA deben demostrar un desempeño consistente y fiable bajo las condiciones previstas, sin que su funcionalidad se degrade con el tiempo. Antes de su despliegue, es obligatorio que los sistemas sean sometidos a pruebas rigurosas para verificar su precisión y garantizar que los resultados que generan sean confiables. Además, en contextos críticos, los sistemas deben ser resilientes y capaces de operar de manera segura incluso en condiciones extremas o impredecibles, lo que es crucial para garantizar su estabilidad y seguridad.

– Los requisitos de documentación y registro son esenciales para asegurar la trazabilidad y rendición de cuentas de los sistemas de IA. Los desarrolladores están obligados a crear documentación técnica detallada que incluya las especificaciones del sistema, los métodos de diseño y desarrollo, y los resultados de pruebas y auditorías[12].

– Garantizar la transparencia y la trazabilidad en los sistemas de IA es un objetivo crucial en el marco del desarrollo y uso responsable de estas tecnologías, pero plantea una serie de desafíos significativos que requieren atención y soluciones innovadoras. Estos desafíos reflejan la complejidad técnica, económica, legal y ética inherente a la implementación de principios de transparencia y trazabilidad en sistemas cada vez más avanzados y autónomos. Abordar estas dificultades es esencial para maximizar los beneficios de la IA al tiempo que se protegen los derechos fundamentales, se fomenta la confianza pública y se promueve la innovación ética.

V. SECTORES CLAVES DEL USO DE LA IA POR LA ADMINISTRACIÓN

– En el ámbito educativo, la IA ofrece un enorme potencial para personalizar el aprendizaje, identificar necesidades específicas de los estudiantes y mejorar la eficiencia en la administración de instituciones educativas. Sin embargo, su uso también plantea desafíos significativos en términos de equidad, privacidad y transparencia.

12. Durante su operación, los sistemas deben mantener un registro detallado de todas sus actividades, incluidas las decisiones automatizadas, los datos utilizados y cualquier evento relevante. Además, esta documentación y los registros deben estar disponibles para las autoridades reguladoras y otras partes interesadas en caso de auditorías o investigaciones, garantizando así un alto nivel de transparencia y control en el uso de la IA.

Los sistemas de IA que se utilizan para personalizar el contenido educativo deben garantizar que sus algoritmos no perpetúen sesgos o discriminen a ciertos grupos de estudiantes. Esto es especialmente importante en contextos donde las decisiones automatizadas, como la asignación de recursos o la evaluación del rendimiento, pueden influir directamente en las oportunidades de los estudiantes. Además, es esencial garantizar que los datos personales de los estudiantes, como sus registros académicos y preferencias de aprendizaje, estén protegidos frente a accesos no autorizados o usos indebidos. La transparencia también juega un papel crucial, ya que los padres, los estudiantes y los educadores deben entender cómo funcionan los sistemas de IA, qué criterios se utilizan para tomar decisiones y cómo pueden cuestionar o apelar resultados que consideren injustos.

– En el sector del transporte, la IA está transformando la manera en que se gestionan y operan los sistemas de movilidad, desde vehículos autónomos hasta sistemas de tráfico inteligentes. Sin embargo, el despliegue de estas tecnologías requiere un marco regulador robusto que garantice la seguridad, la fiabilidad y la equidad. Los vehículos autónomos, por ejemplo, deben cumplir con estándares estrictos de seguridad antes de ser autorizados para operar en vías públicas, lo que incluye pruebas rigurosas en condiciones controladas y simulaciones de escenarios de riesgo. Además, es esencial garantizar que estos vehículos sean capaces de tomar decisiones éticas en situaciones críticas, como en accidentes inevitables, donde la elección de una acción específica podría tener implicaciones significativas para la seguridad de los pasajeros y los peatones.

También es importante abordar las preocupaciones relacionadas con la privacidad, ya que los vehículos autónomos recopilan y procesan grandes cantidades de datos sobre sus usuarios y el entorno. La regulación debe garantizar que estos datos se utilicen de manera responsable y que los usuarios tengan control sobre cómo se recopila y utiliza su información.

– En el ámbito de la seguridad, la IA se utiliza para una amplia gama de aplicaciones, desde la vigilancia y el control de fronteras hasta la detección de actividades sospechosas y la prevención de delitos. Estas aplicaciones pueden mejorar significativamente la eficiencia y la eficacia de las operaciones de seguridad, pero también plantean riesgos considerables para la privacidad y las libertades civiles. Por ejemplo, el uso de cámaras de reconocimiento facial para identificar a personas en espacios públicos puede ser útil para localizar a

ESTUDIOS

En esta obra expertos y académicos de prestigio analizan el impacto de la IA y los retos que supone para la Administración desde diferentes ámbitos jurídicos (contratación, protección de datos, relaciones de consumo, aspectos fiscales, propiedad intelectual, ética, etc.), así como algunos estudios de Derecho comparado (Portugal, Andorra o Cuba) tomando como referencia la entrada en vigor en 2026 de la normativa europea que regula esta materia ya que, para ese momento, toda la estructura pública (y también los operadores privados) han de adaptar sus servicios a esta normativa la cual permite o prohíbe el uso de esta tecnología en función del riesgo que suponga para los ciudadanos). Este trabajo incluye una propuesta de Protocolo para la Administración Local que propone actuaciones coherentes con la normativa europea a la Administración local. En definitiva, es un libro dirigido a los profesionales del Derecho y de otras áreas afines cuya actividad profesional se centre en el uso y explotación de la IA y también para quienes se acercan por primera vez a este tema.

ISBN: 978-84-1085-198-6

UNIVERSITAS Miguel Hernández
DIPUTACIÓN DE ALICANTE
ARANZADI