

## Los riesgos a los derechos humanos por la inteligencia artificial: su intento de mitigación en la EU AI ACT

*The risks to human rights posed by ai:  
their mitigation efforts in the EU AI ACT*

Isabella Taboada Macías

 <https://orcid.org/0009-0003-0254-2348>

Universidad Panamericana. México  
Correo electrónico: itaboada@up.edu.mx

Publicación: 28 de octubre de 2024

DOI: <https://doi.org/10.22201/ijj.24484881e.2025.52.19226>

**Resumen:** Este trabajo tiene por objeto analizar la EU AI ACT que supone el primer gran intento por regular la inteligencia artificial para mitigar riesgos a los derechos humanos, analizando sus antecedentes, su regulación y ofreciendo una valoración.

**Palabras clave:** derechos humanos, inteligencia artificial, legislación.

**Abstract:** This paper aims to analyze the EU AI ACT, which represents the first attempt to regulate AI to mitigate risks to human rights, exploring its background, regulation and providing an assessment.

**Keywords:** human rights, artificial intelligence, legislation.

**Sumario:** I. Introducción. II. Hacia una regulación de la inteligencia artificial. III. La Ley de Inteligencia Artificial de la UA (EU AI ACT). IV. Valoración de la EU AI ACT. V. Referencias.

### I. Introducción

La inteligencia artificial (IA) ha revolucionado diversos aspectos de la vida moderna, desde la salud y la educación hasta la seguridad y el empleo.

Sin embargo, esta tecnología emergente también plantea desafíos significativos para los derechos humanos. La capacidad de la IA para procesar grandes volúmenes de datos y tomar decisiones automatizadas puede, por un lado, potenciar derechos fundamentales como el acceso a la información y la salud; pero, por otro, puede amenazar la privacidad, la igualdad y la autonomía personal.

La intersección entre derechos humanos y la IA ha generado un debate global sobre la necesidad de regular esta tecnología para evitar abusos y garantizar que su desarrollo y uso respeten la dignidad humana. Reconociendo esta necesidad, el Parlamento Europeo legisló en la materia, en la ley conocida como EU AI ACT, en marzo de 2024, que es el objeto de este trabajo.

Dicha legislación es especialmente significativa porque no solo establece un marco legal robusto dentro de la Unión Europea, sino que también sienta un precedente a nivel global. La EU AI ACT se posiciona como un referente clave que influirá en la formulación de políticas de inteligencia artificial en otros países y regiones, promoviendo un enfoque ético y responsable en el desarrollo y uso de esta tecnología.

Para tratar esa ley, se abordará, en primer término, el camino que se siguió hacia la legislación: desde su necesidad hasta el desarrollo de normativas y principios éticos previos; posteriormente, se analizará el contenido de la ley propuesta, pata finalmente ofrecer una valoración crítica de la ley.

## II. Hacia una regulación de la inteligencia artificial

La IA presenta un doble filo en el ámbito de los derechos humanos. Por un lado, puede ser una herramienta poderosa para apoyar y mejorar estos derechos; por otro, plantea riesgos significativos de transgresión. (Hernández, 2023, pp. 215 y ss.)

Lo anterior queda claro analizando derechos en particular. En el caso del derecho a la protección de la salud, la IA puede ser un aliado en tanto facilita diagnósticos precisos, previsión de riesgos, tratamientos personalizados, cirugía robótica y asistencia médica remota. Sin embargo, el uso de datos personales sensibles y la posible falta de control humano sobre decisiones automatizadas plantean preocupaciones serias sobre la integridad y autonomía del paciente. (Andrés Segovia, 2021, pp. 327 y ss.)

La IA también podría coadyuvar a mejorar el acceso a la justicia, pues ayuda a sistematizar información jurídica y predecir decisiones basadas

en precedentes. No obstante, la falta de capacidad para argumentar y garantizar decisiones justas y equitativas puede resultar en inexactitudes y en discriminación. (Nieva, 2018, p. 17) Lo mismo podría decirse en el caso de la seguridad ciudadana, donde la IA puede ser utilizada para el reconocimiento biométrico, el análisis de comportamientos y la búsqueda de personas desaparecidas, pero con el riesgo de abuso en el tratamiento de datos personales y de dependencia de sesgos discriminatorios en la vigilancia predictiva.

En el caso del derecho al trabajo, la IA puede hacerlo más efectivo, facilitando que las personas encuentren empleo de manera más eficiente y equitativa, además de que puede automatizar y mejorar los procesos de selección; pero el riesgo es el mismo: los algoritmos pueden ocultar y perpetuar sesgos discriminatorios. (Pérez López, 2023, pp. 186 y ss.)

De esta forma, aunque la IA ofrece numerosos beneficios para la sociedad, también conlleva riesgos significativos para la dignidad y los derechos humanos. Estos riesgos se intensifican especialmente en grupos vulnerables, como menores, inmigrantes y personas con discapacidad (Valle, 2023, pp. 7 y ss.). Es esencial abordar estos desafíos para asegurar que la IA contribuya positivamente al bienestar humano sin comprometer los derechos fundamentales.

Ante este panorama, desde hace años en el ámbito europeo se consideró necesario regular la IA. La Unión Europea (UE) adoptó un enfoque particular: en lugar de comenzar con normas jurídicas, decidió primero establecer principios éticos sobre la IA. Este enfoque se eligió porque los principios éticos pueden proporcionar una base sólida y flexible que guíe el desarrollo y la implementación de la IA de manera responsable.<sup>1</sup> Al priorizar la ética, la UE buscaba asegurar que cualquier legislación futura estuviera firmemente anclada en valores fundamentales como la dignidad humana, la justicia y la transparencia.

El primer texto del Parlamento Europeo con contenido ético significativo fue su propuesta de carta sobre robótica de 2017. Esta carta establecía que la IA debería regirse por principios éticos como la beneficencia, la no maleficencia, la autonomía del usuario, la justicia, el respeto de los derechos fundamentales, la precaución, la participación, la transparencia, la ren-

---

<sup>1</sup> El Parlamento Europeo sostuvo que eran conscientes de que las normas jurídicas no eran suficientes, y por ello afirmó que era mejor contar con “un marco ético claro, estricto y eficiente que oriente el desarrollo, diseño, producción, uso y modificación de los robots” (Resolución, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica).

dición de cuentas, la seguridad, la reversibilidad de la acción, la privacidad, la maximización de beneficios y la reducción de daños.<sup>2</sup>

El segundo paso lo dio en 2019, cuando aprobó una resolución en la que instaba a la Comisión a revisar y adaptar la legislación europea a la nueva realidad tecnológica desde una perspectiva ética. Esta resolución proponía nuevos principios para complementar la legislación existente y enfatizaba la necesidad de una carta ética de buenas prácticas para la IA.<sup>3</sup>

Los siguientes pasos se dieron en 2020, cuando se emitieron dos resoluciones en las que reconocieron que el marco ético era insuficiente para proteger eficazmente los derechos fundamentales frente a la IA, especialmente en términos de privacidad, autonomía y el desarrollo normal de una sociedad democrática en el ecosistema digital. Por ello, se propuso la aprobación de un par de reglamentos con obligaciones legales uniformes para todos los Estados miembros, y de aplicación directa.<sup>4</sup>

El primer reglamento propuesto señalaba que “los principios éticos comunes solo son eficaces cuando están también asentados en Derecho”,<sup>5</sup> y planteaba un anexo que identificara sectores, usos y fines de alto riesgo para los derechos humanos, tales como el empleo, la educación, la asistencia sanitaria, el transporte, la energía, la seguridad, la defensa, las finanzas y el sector público, incluyendo asilo, migración, control fronterizo, sistema judicial y servicios de seguridad social.

El segundo reglamento propuesto pretendía establecer un régimen de responsabilidad civil, tanto objetiva como subjetiva, que permitiría recla-

---

<sup>2</sup> En dicha resolución, de 16 de febrero de 2017, afirmó que era necesario que una futura regulación jurídica se basara “en los principios de beneficencia, no maleficencia, autonomía y justicia, así como en los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, como la dignidad humana, la igualdad, la justicia y la equidad, la no discriminación, el consentimiento informado, la vida privada y familiar y la protección de datos, así como en otros principios y valores inherentes al Derecho de la Unión, como la no estigmatización, la transparencia, la autonomía, la responsabilidad individual, y la responsabilidad social” (núm. 13).

<sup>3</sup> Resolución, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI)). En los núms. 114-137 de ese documento se establecieron las recomendaciones para la modificación del marco jurídico.

<sup>4</sup> Nos referimos a la resolución 2020/2022(INI) y a la 2020/2015(INI), ambas del 20 de octubre de 2020. En la segunda de estas se afirmó que se requería de “un marco regulador operativo y plenamente armonizado en el ámbito de las tecnologías de IA”, y sugirió que dicho marco adopte la forma de un reglamento y no de una directiva (núm. 3).

<sup>5</sup> Propuesta de reglamento del marco regulador, Considerando Y. Esa propuesta se encuentra en la 2020/2012(INL), de 20 de octubre de 2020.

mar cualquier daño, material e inmaterial, derivado del uso de la IA, incluyendo violaciones de derechos importantes jurídicamente protegidos, como la vida, la salud, la integridad física y la propiedad.<sup>6</sup> También se preveía un anexo que recogería los sistemas de alto riesgo, los cuales estarían sujetos a un régimen de responsabilidad objetiva, mientras que el resto seguiría bajo responsabilidad subjetiva.

Sin embargo, la Comisión Europea decidió ir más allá, y en abril de 2021 presentó una iniciativa de Ley de Inteligencia Artificial, que busca consolidar un marco legal robusto que no solo incorpore principios éticos, sino que también establezca obligaciones jurídicas claras y mecanismos de responsabilidad para proteger los derechos humanos y garantizar el uso seguro y equitativo de la IA.

### **III. La Ley de Inteligencia Artificial de la UA (EU AI ACT)**

El itinerario antes relatado culminó con la aprobación de la legislación en comento, conocida como EU AI ACT, en marzo de 2024, con 523 votos a favor, 46 en contra y 49 abstenciones.<sup>7</sup> Con esta se crea un marco normativo aplicable a todos los proveedores, implantadores, fabricantes, distribuidores y demás usuarios que interactúen con sistema que sean utilizados o desarrollados en la UE. Tiene como objetivo armonizar el desarrollo, el uso y la comercialización de los sistemas de IA en la UE, la prohibición de prácticas de riesgo inaceptable, la determinación de las obligaciones tanto de los desarrolladores, como de los usuarios y/u operadores, la delimitación de las normas de transparencia, supervisión, comercialización, gobernanza, así como las medidas de apoyo a la innovación de nuevas IA.

#### ***1. La clasificación de los sistemas de IA con base en el riesgo de los derechos humanos***

La norma define a los sistemas de IA como “un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y que puede

---

<sup>6</sup> La propuesta de reglamento se encuentra en la Resolución 2020/2014(INL), de 20 de octubre de 2020.

<sup>7</sup> Parlamento Europeo (2024). Artificial Intelligence Act: MEPs adopt landmark law. <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>

mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales” (artículo 3o.), y los clasifica en función de su riesgo hacia los derechos humanos en cuatro categorías: los de riesgo inaceptable, los de riesgo alto, los de riesgo limitado y los de riesgo mínimo para los derechos.

#### *A. Sistemas de riesgo inaceptable para los derechos*

De acuerdo con el artículo 5o. de la ley, son sistemas de riesgo inaceptable aquellos que incluyen prácticas como el despliegue técnicas subliminales que resulten manipuladoras o engañosas en la toma de decisiones del consumidor; los que exploten vulnerabilidades; los sistemas de categorización biométrica y/o evaluación, clasificación y puntuación de persona con el fin de evaluar o predecir el riesgo de que una persona física cometa un delito; los sistemas que busquen inferir emociones de una persona en los ámbitos del lugar de trabajo en de las instituciones educativas (salvo por razones médicas o de seguridad). Esos sistemas quedan prohibidos.

También proscribe la compilación de bases de datos de reconocimiento facial mediante el raspado no selectivo de imágenes faciales de Internet o de grabaciones de CCTV, y la identificación biométrica a distancia “en tiempo real” con fines policiales, a menos que sea estrictamente necesaria para búsqueda específica de víctimas de algún delito como secuestro o trata de personas, para la prevención de alguna amenaza específica, o para la localización de una persona sospechosa de alguna infracción penal.

En esos casos de excepción se requiere de una autorización para operarlos para valorar tanto la naturaleza de la situación (evaluando la magnitud del perjuicio causado en caso de no ser utilizada), como las consecuencias de la utilización para las personas afectadas. Por ello, antes de su aplicación, la policía debe completar una evaluación de impacto sobre los derechos fundamentales y registrar el sistema en la base de datos de la UE (salvo en casos de urgencia) ajustándose a una serie de condiciones temporales, geográficas y personales de las legislaciones nacionales.

#### *B. Sistemas de riesgo alto*

Por otra parte, en la norma se regulan los sistemas de riesgo alto. En estos encontramos aquellos destinados a utilizarse como componente de seguri-

dad y que deba someterse a una evaluación de la conformidad por terceros con arreglo a la legislación de armonización de la UE, así como los sistemas enumerados en el anexo III, que son los relacionados con el uso de datos biométricos, infraestructuras críticas (suministro de agua, gas, calefacción y electricidad), educación y formación profesional, empleo, gestión de trabajadores y acceso al autoempleo, prestación de servicios esenciales, tanto públicos como privados, fuerzas y cuerpos de seguridad (siempre que el uso esté permitido por la legislación nacional), gestión de migración, asilo y control de fronteras, administración de justicia y procesos democráticos (artículo 60.).

En estos casos no hay una prohibición absoluta, pero si una intensa regulación, que incluye que los sistemas deben:

- a) Establecer un sistema de gestión de riesgos que será revisada y actualizada de manera periódica y sistemática a lo largo de todo el ciclo de la vida del sistema de IA (artículo 90.);
- b) Elaborar documentación técnica antes de su comercialización o puesta en servicio para demostrar a la autoridad que el sistema cumple los requisitos establecidos y proporcione a las autoridades nacionales competentes y a los organismos notificados la información necesaria de forma clara y completa (artículo 11);
- c) Dar mantenimiento de registros a fin de garantizar un nivel de trazabilidad del funcionamiento del sistema de IA (artículo 12);
- d) Ser totalmente transparentes en el suministro de información a los empresarios, lo que implica que deberán ser acompañados de instrucciones de uso, cuya información será accesible y comprensible para los usuarios (artículo 13);
- e) Contar con supervisión humana para prevenir o reducir los riesgos a la salud, seguridad o derechos fundamentales; (artículo 14);
- f) Cumplir con los estándares de precisión, robustez y ciberseguridad, y
- g) Los sistemas que hagan uso de técnicas que impliquen el entrenamiento de modelos con datos deberán de llevar a cabo la gobernanza de los datos garantizando su validación y evitando, en medida de lo posible, errores (artículo 10).

Este es un caso muy claro de regulación para respetar los derechos humanos que, como se apuntó anteriormente, pueden ponerse en riesgo con la IA. Especial énfasis se pone en el tema de la seguridad y de la vigilancia,

con el objeto de no vulnerar los derechos a la privacidad y a la intimidad de las personas, sino que, por el contrario, puedan desarrollarse libremente.

### **C. Sistemas de riesgo limitado y mínimo**

Cuando el sistema no supone un riesgo significativo a la salud, seguridad o derechos humanos de las personas, es decir, cuando está destinada a realizar una tarea procedimental limitada, mejorar resultados de una actividad humana o detectar patrones, el proveedor deberá presentar los documentos necesarios para una evaluación y registro antes de comercializarlo o ponerlo en servicio. (artículo 52).

Además, la ley establece las obligaciones de los proveedores e implantadores de sistemas que, de manera enunciativa más no limitativa, incluye disponer de un sistema de gestión de calidad, conservar la documentación y registros generados, garantizar que el sistema se someta al procedimiento de evaluación, cumplir con las obligaciones de registro y transparencia, entre otras (artículos 53 y 54).

Estos modelos, considerados de propósito general, pueden suponer un riesgo sistemático, lo cual es determinado bien mediante una evaluación de si sus metodologías y técnicas son adecuadas; o bien, cuando así lo dispone la comisión de oficio o tras una alerta cualificada de la Comisión Técnica Científica. En este segundo supuesto, la alerta da lugar a que, en respeto a la garantía de audiencia, el proveedor pueda ofrecer pruebas de que no hay un riesgo sistemático, tras lo cual, decidirá la comisión. En cualquier caso, se debe publicar un listado de modelos de IA de propósito general con riesgo sistemático, que debe estar actualizado.

De cualquier manera, sean o no de riesgo sistemático, los proveedores de modelos de IA de propósito general cuentan con una serie de obligaciones, entre las cuales se encuentra elaborar y mantener actualizada la documentación técnica del modelo, proporcionar información y documentación a los proveedores de sistemas de IA que busquen integrar el modelo a sus sistemas, respetar la legislación de la Unión, publicar un resumen detallado sobre el contenido utilizado para entrenar el modelo de IA de propósito general, designar a un representante autorizado y cooperar con la comisión y las autoridades nacionales, entre otras (artículo 53).

A estas obligaciones se les suman otras, en caso de que se trate de un modelo de riesgo sistemático, pues en tal caso los proveedores deben realizar la evaluación del modelo, mitigar los posibles riesgos, documentar y comu-

nicar incidentes graves y garantizar un nivel adecuado de protección de la ciberseguridad (artículo 55).

## ***2. Autoridades, obligaciones***

El paso de la regulación ética a la jurídica supuso la necesidad de normar a las autoridades y sus competencias para la debida implementación de la EU AI ACT. En concreto, en las secciones 4 y 5 del capítulo III, se determina quienes serán las autoridades competentes para notificar y los organismos notificados que se encargarán de establecer y aplicar los procedimientos para la evaluación, designación y notificación de organismos de evaluación.

Asimismo, en el capítulo VII se determina la gobernanza a escala de la Unión, para lo cual se crea la “Oficina Europea de Inteligencia Artificial”, en el seno de la comisión, como encargada de supervisar la aplicación de la ley. Se destaca la función clave de la oficina será la facilitación de la elaboración de códigos de buenas prácticas a nivel europeo, abordando distintas cuestiones como la actualización de información, identificación y gestión de riesgos, y la participación de todos los interesados.

De igual forma, se crea una “Junta Europea de Inteligencia Artificial”, cuyo consejo estará compuesto por un representante de cada Estado miembro (electo por su estado por un periodo de 3 años) y deberán asistir el Supervisor Europeo de Protección de datos y la oficina de AI en calidad de observadores sin tomar parte en las votaciones. Este Consejo deberá de manera enunciativa, contribuir a la coordinación entre autoridades nacionales competentes responsables de la aplicación del reglamento, recopilar y compartir conocimientos técnicos y reglamentarios, asesorar en la aplicación del reglamento, contribuir a la armonización de las prácticas administrativas de los Estados miembros, emitir recomendaciones y dictámenes relativos al reglamento, apoyar a la promoción de la alfabetización en la IA, la conciencia pública y comprensión de beneficios, riesgos, salvaguardias y desechos y obligaciones en relación al uso de sistemas de IA, facilitar el desarrollo de criterios comunes y contribuir y cooperar con otras instituciones, órganos u organismos de la Unión, así como con las autoridades competentes de terceros países.

Por otra parte, se creará un “foro consultivo” para asesorar y proporcionar conocimientos técnicos a la junta y la comisión. Este foro consultivo será designado por la comisión y representarán una selección equilibrada de las partes interesadas (la industria, las nuevas empresas, las PYMES, la sociedad civil y el mundo académico). La Agencia de los Derechos Fundamenta-

les, la Agencia de Ciberseguridad de la Unión Europea, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicación (ETSI) serán miembros permanentes del foro consultivo. También podrá crear subgrupos permanentes o temporales, para examinar cuestiones específicas, relacionadas con los objetivos del reglamento.

Asimismo, contempla un “grupo científico” expertos seleccionados por la comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la inteligencia artificial.

En cualquier caso, los Estados miembros de la Unión tienen también un papel que jugar. Por ello, la ley reconoce que seguirán existiendo espacios propios de regulación de cada Estado, y que cada miembro vele por establecer una autoridad nacional que proporcionen un entorno controlado que fomente la innovación y facilite el desarrollo de los sistemas de IA, mejoren la seguridad jurídica para lograr el cumplimiento normativo, apoyen al intercambio de buenas prácticas, faciliten la cooperación transfronteriza entre las autoridades nacionales y la divulgación pública de información.

#### IV. Valoración de la EU AI ACT

La Ley de Inteligencia Artificial de la UE ha generado opiniones diversas. Por una parte, organizaciones civiles de protección de los derechos humanos en los entornos digitales, como “Access Now”, han expresado su inconformidad con el texto. (Access Now, 2024) Esta organización destaca que, debido a la presión ejercida por la industria tecnológica, la ley presenta numerosas lagunas y excepciones, lo que socava su objetivo de proteger los derechos humanos. Señala, además, que la legislación no prohíbe algunos de los usos más peligrosos de la IA, como el reconocimiento facial en espacios públicos sin un control adecuado, y exime a las autoridades policiales y migratorias de importantes requisitos de transparencia, y esta omisión puede dar lugar a prácticas discriminatorias, y erosionar la confianza pública en la aplicación de estas tecnologías. Además, la ampliación de la exención de seguridad nacional más allá de lo permitido en los tratados de la UE plantea preocupaciones sobre posibles abusos y falta de rendición de cuentas en contextos sensibles como la vigilancia estatal y la seguridad fronteriza, lo cual podría agravar los riesgos en el ámbito migratorio.

Por otro lado, hay quienes consideran que la legislación representa un marco jurídico sólido y exhaustivo. Los defensores de la ley argumen-

tan que adopta un enfoque innovador que permitirá sentar las bases para una regulación integral de la inteligencia artificial. Destacan aspectos positivos como la clasificación de los sistemas de IA por niveles de riesgo, que establece requisitos específicos y proporcionales para diferentes aplicaciones, promoviendo así un uso seguro y ético de la tecnología. Sin embargo, también reconocen que la ley presenta áreas de mejora, particularmente en la falta de regulación del uso de la IA en el ámbito militar, un aspecto crítico dado el potencial uso indebido de estas tecnologías en conflictos armados y operaciones bélicas, lo que podría tener implicaciones graves para la seguridad internacional y los derechos humanos. (Burlacu, F. y Lută, G., 2023)

Además, existen preocupaciones más específicas en diversos sectores. En el ámbito del derecho de daños, se debate cómo la ley aborda la responsabilidad y compensación en casos de perjuicio causado por sistemas de IA, lo que podría complicar la protección de los derechos de los afectados (Chamberlain, J., 2023). En el sector de la robótica, se señala que la legislación no contempla de manera suficiente los desafíos éticos y de seguridad que surgen con el desarrollo y despliegue de robots avanzados, lo cual es crucial para prevenir riesgos asociados con la autonomía y la toma de decisiones por parte de las máquinas (Gallese Nobile, 2023). En cuanto a los sistemas eléctricos, se ha planteado que la integración de la IA expone cuestiones sobre la seguridad y la resiliencia de infraestructuras críticas, y la ley aún no proporciona un marco adecuado para mitigar posibles amenazas en este campo (Niet, I., van Est, R., y Veraart, F., 2021).

Desde mi perspectiva, la Ley de Inteligencia Artificial de la UE debe ser valorada positivamente como la primera legislación de este tipo en el mundo. Este logro es significativo porque establece un precedente global para la regulación de la inteligencia artificial. Aunque no es perfecta, representa un primer paso crucial en la dirección correcta.

La ley pone énfasis en el respeto a la dignidad de las personas, y eso es algo que debe celebrarse. Teniendo claridad en ese valor, pueden desprendérse una serie de principios generales regulatorios que garanticen los derechos humanos. Entrar en más detalles puede ser complicado por la naturaleza compleja y en rápida evolución de la IA. Es necesario que la regulación sea flexible y capaz de adaptarse a los cambios, garantizando que los derechos sean el auriga de la regulación.

No podemos perder de vista que se trata de una regulación pionera, y por ello la UE ha asumido un reto considerable: regular una tecnología en rápida evolución que presenta desafíos técnicos, éticos y sociales complejos.

La complejidad de esta tarea no debe subestimarse: la IA es una tecnología multifacética que afecta a múltiples sectores y aspectos de la vida cotidiana, y su regulación requiere un equilibrio delicado entre fomentar la innovación y proteger los derechos humanos.

Es natural que, como primera ley de su tipo, la legislación presente lagunas y áreas que requieran refinamiento. Sin embargo, su principal valor radica en haber abierto un debate menos abstracto sobre cómo debe regularse la inteligencia artificial. Este debate es esencial no solo para perfeccionar la propia ley, sino también para guiar futuras legislaciones a nivel nacional en los distintos estados miembros de la UE y en otras naciones. La ley ha proporcionado un marco sobre el cual se pueden construir normas más detalladas y específicas, y la crítica constructiva y el debate público serán fundamentales para su evolución y mejora continua.

La implementación de esta ley permitirá identificar áreas de oportunidad y aspectos que necesitan ajustes o clarificaciones. La práctica revelará cómo los principios generales pueden aplicarse en contextos específicos y cómo los distintos actores, desde gobiernos hasta empresas y ciudadanos, interactúan con la legislación.

El debate en torno a la EU AI ACT es esencial no solo para identificar y corregir sus deficiencias, sino también para enriquecer la conversación sobre la vigencia de los derechos humanos en entornos digitales. Es fundamental que en todo momento se priorice la dignidad y los derechos de las personas. La inteligencia artificial tiene el potencial de transformar radicalmente nuestras vidas, pero también presenta riesgos significativos si no se maneja con cuidado.

## V. Referencias

- Access Now (2024), The EU AI Act: a failure for human rights, a victory for industry and law enforcement. <https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/>
- Andrés Segovia, B. (2021). El reinicio tecnológico de la inteligencia artificial en el servicio público de salud. *Ius et Scientia*, 7(1).
- Burlacu, F. y Lută, G. D. G. (2023). The crucial importance of the European Union AI Act as the world's first regulation on artificial intelligence. *Journal of Information Systems & Opera-*

- tions Management. <https://www.proquest.com/scholarly-journals/crucial-importance-european-union-ai-act-as/docview/2973458065/se-2>
- Chamberlain, J. (2023). The risk-based approach of the European Union's proposed artificial intelligence regulation: some comments from a tort law perspective. *European Journal of Risk Regulation*. <https://doi.org/10.1017/err.2022.38>
- Gallese Nobile, C. (2023). Regulating smart robots and artificial intelligence in the European Union. *Journal of Digital Technologies and Law*, 1(1), 33-61. <https://doi.org/10.21202/jdtl.2023.2>
- Hernández, M. (2023). Los retos constitucionales de la inteligencia artificial. Prospectiva, debilidades y fortalezas de los paradigmas vigentes, en Soberanes, J. y Garduño, G., *La interacción de las redes sociales, la tecnología y los derechos humanos*. Eunsa.
- Niet, I., Van Est, R. & Veraart, F. (2021). Governing AI in electricity systems: reflections on the EU artificial intelligence Bill. *Frontiers in Artificial Intelligence*, (4). <https://doi.org/10.3389/frai.2021.690237>
- Nieva, J. (2018). *Inteligencia artificial y proceso judicial*, Marcial Pons.
- Pérez López, J. I. (2023). Inteligencia artificial y contratación laboral. *Revista de estudios jurídico-laborales y de seguridad social (REJLSS)*, (7), 186-205.
- Valle Escolano, R. (2023). Inteligencia artificial y derechos de las personas con discapacidad. *Revista Española de Discapacidad*, II(1).



## Cómo citar

### Sistema IIJ

Taboada Macías, Isabella, "Los riesgos a los derechos humanos por la inteligencia artificial: su intento de mitigación en la EU AI ACT", *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, México, vol. 26, núm. 52, enero-junio de 2025, e19226. <https://doi.org/10.22201/ijj.24484881e.2025.52.19226>

### APA

Taboada Macías, I. (2025). Los riesgos a los derechos humanos por la inteligencia artificial: su intento de mitigación en la EU AI ACT. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, 26(52), e19226. <https://doi.org/10.22201/ijj.24484881e.2025.52.19226>