

# “Inteligencia Artificial y Derechos Humanos – el rol de los Defensores del Pueblo”

**Juan Belikow**

***Primer encuentro de la FIO sobre IA y DDHH  
Santa Fe, Argentina - 1 de agosto de 2023***



Lo lindo

# ¿Qué es la IA?

***Es simulación de la inteligencia humana en máquinas programadas para pensar y actuar como humanos. Una rama de la informática que tiene como objetivo crear agentes inteligentes capaces de percibir su entorno, razonar, aprender de la experiencia y tomar decisiones para lograr objetivos específicos.***

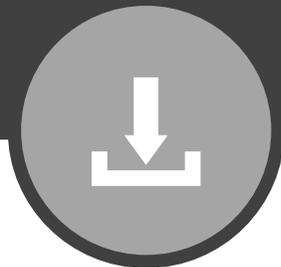
## **IA estrecha/débil**

Diseñada para realizar tareas específicas y sobresalir en un dominio limitado. *Siri, Alexa, sistemas de recomendación de plataformas on-line y algoritmos de reconocimiento de imágenes*



Abarca diversas técnicas, como el aprendizaje automático, el procesamiento del lenguaje natural, la visión por computadora, la robótica y los sistemas expertos.

El aprendizaje automático ha sido fundamental para impulsar muchas aplicaciones de IA al permitir que las máquinas aprendan de los datos y mejoren su rendimiento a lo largo del tiempo sin estar programadas explícitamente para cada tarea.



## **IA general/fuerte**

Forma teórica de IA que posee inteligencia similar a la humana y puede comprender, aprender y adaptarse. *Aun no existe, pero es tema de investigación y especulaciones*

- ✓ *El potencial de la IA es vasto y abarca múltiples industrias, incluidas la salud, las finanzas, la educación, el transporte, el entretenimiento y más. Tiene la capacidad de transformar diversos procesos, optimizar la toma de decisiones y mejorar la eficiencia y la productividad.*
- ✓ *Sin embargo, la IA también plantea importantes consideraciones éticas, sociales y económicas, como la privacidad de los datos, los sesgos, el desplazamiento laboral, la transparencia y la responsabilidad.*
- ✓ *Conforme la IA avanza, se vuelve crucial lograr un equilibrio entre sus beneficios y desafíos para garantizar su desarrollo responsable y ético para en beneficio de la sociedad.*



Lo malo

# ***Riesgos para los DDHH de la IA***

- Privacidad y protección de datos
- Discriminación y sesgo
- Transparencia y responsabilidad (*accountability*)
- Sistemas de armas autónomas
- Empleo y derechos laborales
- Libertad de expresión
- Vigilancia y monitoreo masivo
- Autonomía y toma de decisiones
- Vulnerabilidades de seguridad y de hacking
- Acceso e inclusión

# ***Desafíos éticos de la IA***

- Sesgo y equidad
- Transparencia y explicabilidad
- Autonomía y responsabilidad
- Desplazamiento laboral e impacto económico
- Armas autónomas
- Manipulación y desinformación
- Alineación y control de valores
- Adicción e influencia conductual
- Desigualdad socioeconómica
- IA en la vigilancia y la privacidad

# ***Preocupaciones de sesgo relacionadas con la IA***

- Sesgo de datos
- Sesgo algorítmico
- Equidad y discriminación
- Sesgo de género
- Sesgo racial
- Disparidades en la atención médica
- Sistemas de recomendación
- Sesgo lingüístico
- Implicaciones de privacidad
- Bucles de retroalimentación

- ✓ *Abordar los riesgos de DDHH y los desafíos éticos de la IA requiere un esfuerzo de colaboración entre los gobiernos, los organismos reguladores, los desarrolladores y los investigadores de la IA y la sociedad civil.*
- ✓ *Sólo con un enfoque inclusivo y multidisciplinario de la gobernanza de la IA podremos aprovechar su potencial salvaguardando los DDHH y la dignidad de las personas.*
- ✓ *Las prácticas responsables de IA, junto con los marcos legales y regulatorios, pueden ayudar a garantizar que la IA se desarrolle y despliegue de manera respetuosa de los DDHH, promueva la equidad y evite perpetuar sesgos dañinos.*



Lo feo

# ***Preocupaciones de privacidad relacionadas con la IA***

- Recopilación y almacenamiento de datos
- Consentimiento informado
- Violaciones de datos y seguridad
- Sesgo algorítmico
- Vigilancia y monitoreo
- IA en el cuidado de la salud
- Reconocimiento de voz y voz
- Seguimiento de ubicación
- Uso compartido de terceros
- Retención de datos

*Abordar las preocupaciones de privacidad requiere:*

- ✓ Un enfoque integral, que involucre principios de privacidad por diseño, técnicas de anonimización de datos y leyes (y regulaciones) robustas de protección de datos.*
- ✓ Implementar prácticas sólidas de gobernanza de datos, proporcionar políticas de privacidad claras y ofrecer mecanismos para que las personas ejerzan sus derechos de datos.*
- ✓ Fomentar la transparencia en los procesos de toma de decisiones de IA que puedan generar confianza entre los usuarios con respecto a cómo se utilizan y procesan sus datos.*

# ***Riesgo de puntuación social en IA***

- Invasión de la privacidad
- Falta de transparencia
- Resultados discriminatorios
- Control social y daño a la reputación
- Acceso limitado y desigualdad
- Falta de debido proceso y reparación
- Normalización de la vigilancia
- Uso indebido de datos
- Riesgos de seguridad de datos

*Abordar los riesgos de la puntuación social en IA requiere:*

- Un equilibrio cuidadoso entre el avance tecnológico y la salvaguardia de los derechos individuales y los valores sociales.*
- Marcos regulatorios que priorizan la protección de la privacidad, la transparencia y la equidad para garantizar el despliegue responsable de los sistemas de puntuación social.*
- Un diálogo abierto y la participación pública para abordar las implicaciones éticas y sociales de la puntuación social, y para garantizar que las tecnologías de IA se alineen con los intereses y valores más amplios de la sociedad.*

A digital eye with a blue and green iris, surrounded by binary code and technical text. The eye is the central focus, with a complex, multi-layered iris. The background is dark with various digital elements: binary code (0s and 1s) scattered throughout, some in white and some in blue. There are also some technical-looking strings of text, such as "IMG", "otcer te", "439", "image:", and "100 101010101001". The overall aesthetic is futuristic and high-tech.

Volvamos a lo lindo

## ***Papel del Defensor del Pueblo en la mitigación de esos riesgos...***

Los Defensores del Pueblo pueden desempeñar un papel crucial realizando:

- Monitoreo y evaluación
- Investigación y tramitación de reclamaciones
- Promoción de la transparencia y de la rendición de cuentas
- Orientación y promoción de políticas
- Desarrollo de capacidades y capacitación
- Promoción de la inclusión y la no discriminación

## ***... y cómo pueden usar la IA para enfrentar esos desafíos***

y también pueden aprovechar el potencial de las tecnologías de IA para su trabajo en esta materia, por ejemplo:

- ❖ Usar la IA como herramienta de auditoría
- ❖ Crear sistemas de alerta temprana y reacción rápida
- ❖ Manejo de quejas asistido por IA
- ❖ Análisis de datos y perspectivas
- ❖ Marcos éticos de IA

# ***¿Qué pueden hacer los Defensores del Pueblo para proteger al pueblo de los riesgos de la IA y los abusos contra los DDHH relacionados con la IA?***

- Evaluación proactiva de la IA
- Monitoreo de las implementaciones de IA
- Investigación de quejas relacionadas con la IA
- Promover la transparencia
- Abordar el sesgo y la discriminación
- Colaboración con expertos en IA
- Cooperación internacional
- Protección de denunciantes
- Involucrar a la sociedad civil

# Medidas de la UE para mitigar los riesgos y los desafíos que plantea la IA

- ✓ Reglamento General de Protección de Datos (GDPR)
- ✓ Ética en la IA
- ✓ Marco de Gobernanza de la IA
- ✓ Evaluación de Impacto de Derechos Fundamentales
- ✓ Etiquetado de Sistemas de IA
- ✓ Fomento de la Investigación Responsable en IA
- ✓ Asesoramiento de Expertos
- ✓ Revisión de la Ley de Responsabilidad del Producto
- ✓ Cooperación Internacional
- ✓ Apoyo a la Investigación en Ética y DDHH en IA

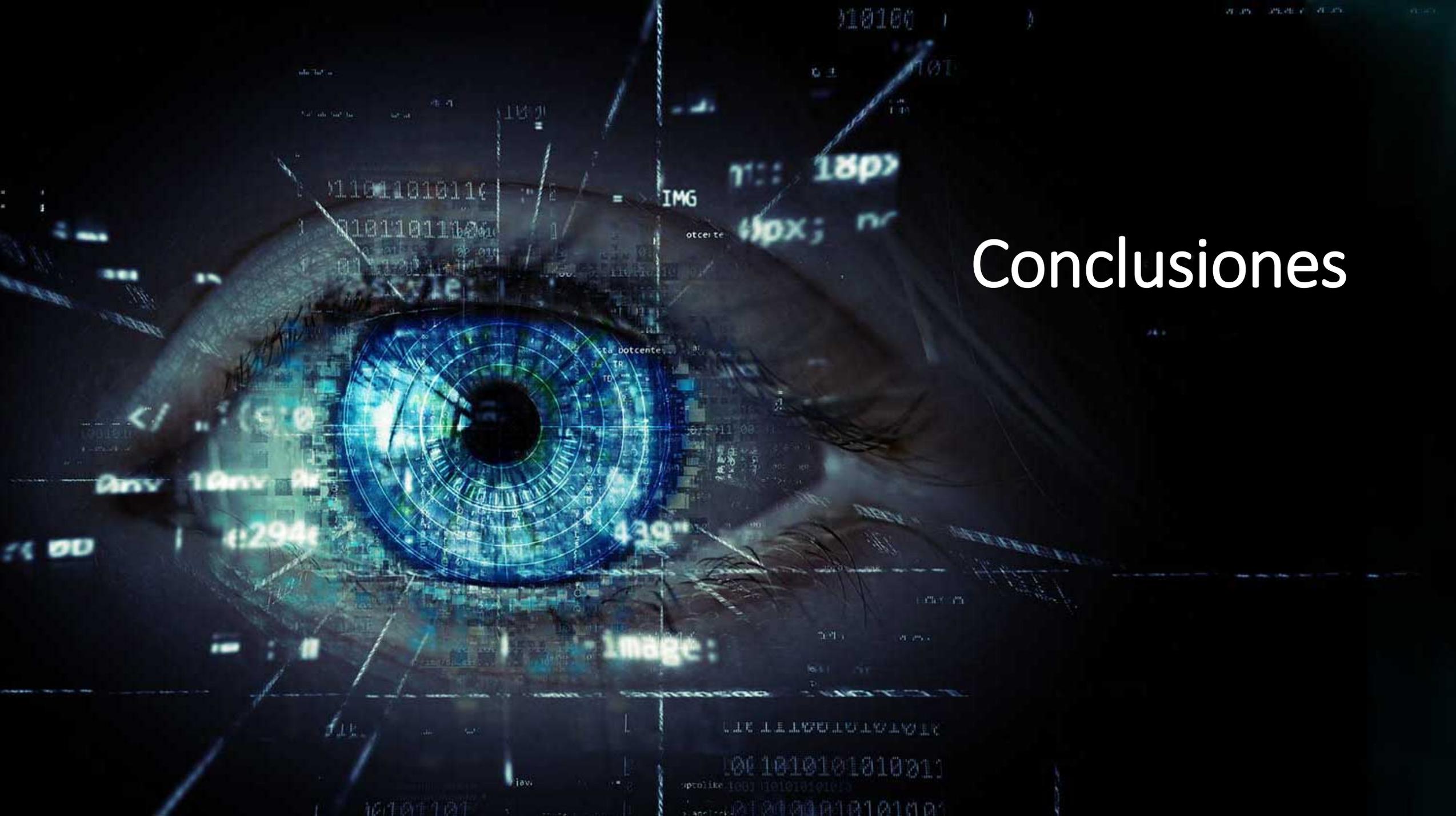
# **Ley sobre la IA de 2021 del Parlamento Europeo: *diferentes normas para diferentes niveles de riesgo***

Se establecen obligaciones para proveedores y usuarios en función del nivel de riesgo de la inteligencia artificial.

- ❑ **Riesgo inaceptable** (prohibidos): sistemas considerados una amenaza para las personas - (manipulación cognitivo-conductual; puntuación social; identificación biométrica remota en tiempo real, policiamiento predictivo)
- ❑ **Alto riesgo**: sistemas que afecten negativamente la seguridad o los derechos fundamentales
- ❑ **IA generativa** (ChatGPT, Bard)
- ❑ **Riesgo limitado**

## *Las Defensorías del Pueblo pueden:*

- ✓ Predicar con el ejemplo y mitigar eficazmente los riesgos para los DDHH de la IA adoptando la IA de manera responsable dentro de sus propias operaciones y utilizarla como una herramienta para la supervisión y la evaluación.*
- ✓ Crear un enfoque holístico e impactante para garantizar el desarrollo y la implementación ética y centrada en el ser humano de las tecnologías de IA colaborando con otras partes interesadas, incluidos los gobiernos, las organizaciones de la sociedad civil y el sector privado.*
- ✓ Proteger de manera proactiva a los ciudadanos de los riesgos de IA y los abusos contra los DDHH.*
- ✓ Oficiar de guardianes diligentes, asegurando que las tecnologías de IA se aprovechen de manera responsable y ética, y que se defiendan los DDHH y la dignidad de las personas frente a los avances tecnológicos.*



# Conclusiones

# ***Principales desafíos de la IA para el ciudadano que debe atender la Defensoría del Pueblo***

- Sesgos y Discriminación
- Falta de transparencia y explicabilidad
- Violación de la privacidad
- Abuso de poder de las empresas privadas
- Responsabilidad y responsabilización
- Seguridad y ciberataques
- Equidad y acceso a la justicia
- Desafíos éticos
- Protección de datos y privacidad
- Pérdida de control
- Capacitación y alfabetización digital

# Amenazas emergentes y la IA

- **Acoso y amenazas en línea:** la IA utilizada para facilitar el acoso en línea, con graves consecuencias para la seguridad emocional y psicológica.
- **Delitos cibernéticos:** organizaciones criminales recurren a la IA para cometer delitos.
- **Desinformación y propaganda:** grupos radicales y extremistas aprovechan la IA para propagar desinformación y propaganda lo que socava la seguridad y la cohesión social.
- **Suplantación de identidad:** con propósitos fraudulentos o criminales.
- **Reconocimiento facial y vigilancia:** infringen derechos civiles, la seguridad y la privacidad del ciudadano al monitorear sus actividades sin su consentimiento. Los criminales recurren a la IA, al *hackeo* de las cámaras de vigilancia y a la información disponible en las redes sociales para realizar tareas de inteligencia sobre sus blancos y víctimas.
- **Protección de datos personales:** La interconexión de la IA y la recopilación masiva de datos personales aumentan los riesgos de violación de la privacidad y el uso indebido de la información.



Bonus track

# ***La IA puede apoyar el trabajo del Defensor del Pueblo***

- Análisis de datos y reconocimiento de patrones
- Gestión automatizada de casos
- Procesamiento del lenguaje natural (NLP)
- *Chatbots* y asistentes virtuales
- Análisis predictivo
- Análisis de sentimiento
- Seguridad de datos y cumplimiento de la privacidad
- Traducción de idiomas
- Detección de fraudes
- Sistemas de apoyo a la toma de decisiones
- Asignación de recursos y gestión de la carga de trabajo
- Aprendizaje continuo

- *A lo largo de esta conferencia, tendremos el privilegio de interactuar con distinguidos expertos, académicos y formuladores de políticas que compartirán sus ideas y experiencias.*
- *Juntos, exploraremos las mejores prácticas, estudios de casos y lecciones aprendidas, con el objetivo de inspirar estrategias efectivas para que los países iberoamericanos naveguen por el panorama de la IA mientras salvaguardan los derechos de sus ciudadanos.*
- *A medida que nos embarcamos en este viaje esclarecedor, recordemos que los avances en IA tienen el potencial de impulsar un cambio positivo en todas las sociedades.*
- *Sin embargo, es nuestra responsabilidad como guardianes de los DDHH asegurarnos de andar con cuidado, aprovechar las oportunidades y mitigar los riesgos.*



Gracias por su atención!

[jbelikow@hotmail.com](mailto:jbelikow@hotmail.com)