

ANDREW TRASK

Científico investigador en DeepMind y líder de OpenMined impulsando IA con privacidad

---

- Experto en IA con preservación de privacidad, aprendizaje federado, computación segura y gobernanza
- Fundador y líder de OpenMined, comunidad global de código abierto con miles de miembros
- Autor de “Grokking Deep Learning” y educador comprometido con la difusión del conocimiento en IA
- Colaborador con sectores financieros, salud, gobierno y académico
- Orador visionario que equilibra rigor técnico con ética y gobernanza aplicables

---

Andrew utiliza la inteligencia artificial para explorar bases de datos de disciplinas diversas y forjar colaboraciones nuevas e inesperadas.

Es Científico Investigador Senior en DeepMind, donde estudia la relación entre privacidad e IA, y es Fundador y Líder de OpenMined, una comunidad de código abierto con más de 12.000 investigadores, ingenieros y entusiastas dedicada a lograr que los conceptos y herramientas necesarios para la IA con preservación de privacidad lleguen a una adopción masiva.

Andrew ha trabajado con fondos de cobertura, bancos de inversión, redes de salud y organismos de inteligencia gubernamental en el desarrollo de soluciones de IA.

También es un apasionado educador de IA, con un gran interés en hacer que las ideas complejas sean fáciles de aprender. Es autor del libro Grokking Deep Learning, instructor en el programa Nanodegree de Deep Learning de Udacity, y autor del popular blog de deep learning “i am trask”. Asimismo, es miembro del Grupo de Trabajo de Privacidad de las Naciones Unidas, donde promueve la concienciación y reduce las barreras de entrada al uso de análisis con preservación de la privacidad en el sector público.

“En la década de 1960, el gobierno de Estados Unidos intervino para crear el ARPANET, democratizando el acceso a las supercomputadoras más potentes del país, porque solo un grupo limitado de investigadores tenía acceso a ellas. Hoy, el gobierno de Estados Unidos interviene para crear el NAIRR, democratizando el acceso a los mayores recursos de IA del país, incluidas las supercomputadoras más avanzadas, porque solo un número limitado de investigadores tiene acceso a ellas. Y con la promesa del NAIRR, el futuro de la IA será democrático, la innovación estadounidense florecerá, y es un honor ser parte de ello.” — Andrew Trask, Director Ejecutivo de OpenMined.

En sus conferencias, Andrew combina un profundo entendimiento técnico con perspectivas visionarias sobre gobernanza, ética y responsabilidad social de la IA. Sus audiencias van desde ingenieros y científicos de datos hasta responsables de políticas públicas, ejecutivos e innovadores interesados en comprender cómo construir sistemas inteligentes que respeten la privacidad y los derechos humanos.

TEMAS

Andrew adapta cada presentación a las necesidades de su audiencia y no se limita a los temas listados a continuación. Por favor, consúltenos sobre cualquier tema que sea de su interés:

- Inteligencia Artificial
- Privacidad, seguridad y gobernanza en inteligencia artificial
- IA y aprendizaje profundo
- IA segura, ética y con preservación de la privacidad
- Gobernanza, ética y responsabilidad social de la IA

PROGRAMAS

Construyendo una inteligencia artificial segura

Andrew presenta en detalle las técnicas más importantes en inteligencia artificial segura, con preservación de la privacidad y gobernanza multiusuario. Comienza con una visión sobria y actualizada del estado de la seguridad en IA, la privacidad de los usuarios y la gobernanza de la IA, antes de introducir algunas de las herramientas fundamentales de la seguridad técnica en IA: cifrado homomórfico, computación multipartita segura, aprendizaje federado y privacidad diferencial. Concluye con una demostración del proyecto de código abierto OpenMined que ilustra cómo entrenar una red neuronal profunda mientras tanto los datos de entrenamiento como el modelo permanecen en un estado seguro y cifrado durante todo el proceso.

IA con preservación de la privacidad

Andrew aborda ideas como la Privacidad Diferencial y la Computación Multipartita Segura, y explica cómo entran en juego.

Muchas industrias están limitadas por las regulaciones de los datos privados y, como respuesta a la necesidad de mayor privacidad en la IA, se han desarrollado tres técnicas de vanguardia con un enorme potencial para el futuro del aprendizaje automático en el sector salud: aprendizaje federado, privacidad diferencial y computación cifrada. Estas técnicas modernas de privacidad permitirían entrenar modelos sobre datos cifrados provenientes de

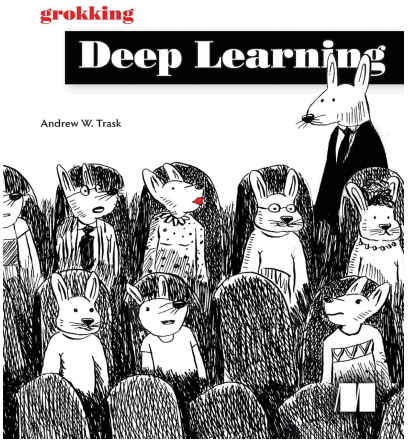
múltiples fuentes, sin necesidad de compartir los datos.

¿Qué es la Privacidad Significativa?

Andrew explica cómo resolver las mayores preocupaciones de privacidad en el mundo utilizando diversas tecnologías de vanguardia en preservación de la privacidad, como el aprendizaje automático con preservación de privacidad.

PUBLICACIONES

Libros



GROKKING DEEP LEARNING

CONDICIONES

- **Viaja desde:** Oxford, Reino Unido
- **Rangos:** Consultar tarifa con HiCue Speakers
