



La otra cara de la moneda, IA responsable: practicidad vs ética

Kevin Miller
CTO de IFS

En noviembre de 2022, OpenAI lanzó ChatGPT-3 para uso público, seguido de ChatGPT-4 el 14 de marzo de 2023, después de la explosiva popularidad de GPT3.

El 29 de marzo, más de 1.100 líderes tecnológicos, incluidos Elon Musk y Steve Wozniak, firmaron una carta abierta pidiendo a todos los laboratorios de IA que detuvieran la investigación y el desarrollo durante seis meses. Poco después, Italia se convirtió en el primer país en prohibir el uso de ChatGPT, seguido por la Unión Europea y China anunciando sus propios planes para regular la IA. El debate sobre la IA ética, y el temor de que la humanidad fuera aniquilada por la inteligencia incognoscible de nuestra propia creación, se reavivó una vez más.

Cuando pensamos en IA responsable, lo primero que nos viene a la mente es cómo afecta a las empresas tecnológicas: cómo se regulará el desarrollo de la IA y qué desarrollos traerá consigo. Ahora que las máquinas inteligentes se están volviendo más omnipresentes en toda la economía, el debate se sumerge en cómo afecta a quienes están fuera de la tecnología.

Para muchos, en una industria como la fabricación, por ejemplo, las principales preocupaciones no son si la IA tendrá un efecto directo. Más bien, se trata de poder com-

» Cuando pensamos en IA responsable, lo primero que nos viene a la mente es cómo afecta a las empresas tecnológicas

prender los consejos y las decisiones que toman los modelos de IA, además de ser capaces de detectar malware, a medida que las organizaciones se integran y confían cada vez más en ella.

USOS DE LA IA EN EL MUNDO REAL

El escenario ideal para la IA es lograr un mundo mejor. Por ejemplo, en el sector fabricante o de utilities, la IA puede ayudar a liberar tiempo y recursos valiosos al automatizar las cargas de trabajo, tomar decisiones comerciales óptimas y agilizar las operaciones.

El mantenimiento predictivo es solo un ejemplo de dónde la IA puede consolidarse como una herramienta para simplificar las operaciones de servicio de campo con la identificación de las necesidades de mantenimiento de la maquinaria antes de que se implemente el equipo de servicio. Esto permite a las empresas recuperar el tiempo que anteriormente se habría dedicado a diagnosticar un problema y viajar de ida y vuelta al sitio, que ahora se puede gastar en tareas más importantes o simplemente hacerlo más rápido.

¿QUÉ ES LA IA EXPLICABLE Y POR QUÉ ES CLAVE PARA UNA IMPLEMENTACIÓN EXITOSA DE LA IA?

Cuando se trata de IA responsable, hay dos aspectos importantes a considerar. El primero es el aspecto práctico: ¿está tomando las decisiones correctas por las razones correctas?

Tener una IA explicable es muy importante para comprender por qué toma las decisiones que toma, y por qué, si toma una decisión equivocada, continuó ese camino. A menudo, esto se convertirá en un ciclo en el que el aprendizaje automático alimenta la IA, y la IA produce más datos para el modelo de aprendizaje automático. El razonamiento defectuoso contaminará la salida, lo que resultará en datos inutilizables y una toma de decisiones poco fiables.

En el otro lado de la moneda, el aspecto ético se centra en aquellas preocupaciones de ciberseguridad que rodean a la IA. El ransomware presenta un problema importante para cualquier sistema de IA: además de simplemente entregar malware para cerrar un negocio, ¿qué pasa si se usa para fines más insidiosos y discretos?

Si el malware corrompe los datos en un sistema de IA, por ejemplo, deformando el algoritmo, puede llevar a consecuencias más desastrosas, como dañar los productos y la reputación de la empresa.

POR QUÉ LA MAYOR AMENAZA DE LA IA ES EL MALWARE

Cuanto más autónomos e inteligentes se vuelven los sistemas de IA, mayor es el riesgo de que una entidad maliciosa se infiltre y corrompa sin apagarla por completo, por lo que es menos probable que se detecte y corrija de manera oportuna. La falta de intervención humana le da al malware, cuyo objetivo es propagar un ataque y propagarse rápidamente a través de todo un sistema de TI, más oportunidades de pasar desapercibido.

La ciberseguridad, y especialmente los principios de confianza cero y aislamiento, se vuelven críticos para el uso seguro y responsable de la IA. Desde asegurarse de que el software produzca el nivel correcto de pruebas y auditorías, hasta separar los deberes y los conjuntos de permisos para cada tarea o usuario. De esta manera, la IA práctica y ética van de la mano hacia la creación de una IA responsable, que luego se puede utilizar según lo previsto para impulsar la toma de decisiones empresariales. Por supuesto, la pregunta sigue siendo ¿cómo nos aseguramos de que la IA que estamos desarrollando sea ética y práctica?

ChatGPT ha demostrado ser más eficiente y capaz con cada interacción, mientras gana popularidad al mismo tiempo. Si bien el miedo a lo desconocido siempre estará presente y, por razones válidas, es muy poco probable que las personas dejen de fabricar nuevas herramientas de IA, de la misma manera que continuamos explorando el espacio o las profundidades del mar. En cambio, se trata de asegurarnos de que entendemos cómo funciona, hacer que funcione para nosotros y, además, protegerlo contra ataques maliciosos de malos actores. ■

» El mantenimiento predictivo es solo un ejemplo de dónde la IA puede consolidarse como una herramienta para simplificar las operaciones de servicio de campo con la identificación de las necesidades de mantenimiento de la maquinaria antes de que se implemente el equipo de servicio