OPINIÓN / DESPUÉS DE LA PANDEMIA

Inteligencia artificial: ¿hacerla o comprarla?

por Enrique Dans

22 mayo, 2024 - 02:09

GUARDAR

Cada vez son más los directivos que, en mis clases y conferencias, me expresan preocupaciones acerca de la propiedad de la información corporativa o personal que introducen **en modelos de inteligencia artificial generativa como ChatGPT, Gemini y otros.**

La teoría es clara: dado que las iteraciones de un modelo de inteligencia artificial generativa pueden pasar a formar parte de su archivo y llegar incluso a aparecer en respuestas a otros usuarios, en general, no se considera seguro **introducir información confidencial o corporativa** en algoritmos de inteligencia artificial generativa.

Las razones son múltiples: en primer lugar, **los proveedores de inteligencia artificial pueden registrar las interacciones para diversos fines,** que van desde la mejora del modelo, a su depuración o al cumplimiento de las políticas de uso. Además, la mayoría de los proveedores de servicios de IA tienen términos de servicio específicos que aconsejan no compartir información sensible o confidencial. Generalmente, se recomienda a los usuarios evitar ingresar cualquier información que pueda comprometer la privacidad personal o corporativa.

Aunque algunos proveedores de IA afirman que los datos de los usuarios no se utilizan para su entrenamiento posterior, las políticas pueden variar. Sin embargo, que una compañía prohiba taxativamente el uso de algoritmos generativos a sus trabajadores tiene un efecto secundario: que

esos trabajadores, además de pasar a ser menos productivos en muchas de sus tareas, **pasan a tener un menor valor al no desarrollar experiencia en ese ámbito.**

Eso ha llevado a que algunas compañías como Microsoft, con amplia experiencia en entornos corporativos, ofrezca versiones de su algoritmo de inteligencia artificial generativa Copilot que aseguran que los datos no se compartan fuera de la compañía. Microsoft implementa varias medidas de protección de datos para su Copilot en servicios como Microsoft 365 y Dynamics 365, intentando con ello obtener una ventaja en un mercado que lleva años dominando.

> *No se considera seguro introducir información confidencial o corporativa en algoritmos de inteligencia artificial generativa*

Otro movimiento cada vez más pujante es el que están llevando a cabo compañías como Huawei y otras compañías tecnológicas chinas con la llamada *AI in a box*: un conjunto de algoritmos con sus procesadores y otros componentes de *hardware* necesarios, como el almacenamiento, que son ofrecidos a compañías para que desplieguen en ellos sus propios modelos de manera completamente estanca, sin depender del proveedor.

Por el momento, Huawei ofrece ese tipo de soluciones a compañías chinas, en ocasiones vinculadas a sus propias soluciones de computación en nube privada, un mercado que domina en China —mientras otras compañías tecnológicas como Alibaba, Tencent o Baidu dominan la nube pública. Sin embargo, algunas compañías opinan que la amortización del uso de un modelo de inteligencia artificial generativa precisa de un uso muy intenso,

y que en muchos casos, el intento de obtener la seguridad total que ofrece un entorno completamente cerrado y privado **conlleva un coste difícil de justificar.**

De una u otra manera, la realidad es que las compañías necesitan empezar a pensar cómo incorporar la inteligencia artificial en sus procesos, y de hecho, ya hemos incluso empezado a ver casos de empresas que consideran esa responsabilidad como crítica y no dudan en elevarla a su *C-suite*, con la designación de los llamados CAIO, *Chief AI Officer*. que se encargan de garantizar la responsabilidad, el liderazgo y la supervisión de la tecnología.

¿Qué pasos debería dar tu compañía con respecto a la inteligencia artificial? En primer lugar, es importante entender de dónde venimos. Las posibilidades de una compañía para competir en el futuro va a depender fundamentalmente de su capacidad para dotarse de una "manguera de datos", de una forma de **generar datos a partir de su actividad que puedan ser directamente utilizados para entrenar algoritmos.**

Que esos algoritmos sean propios, creados por la propia compañía, o por la *big tech* de turno dependerá, lógicamente, de muchas cosas. Nadie tiene mejores datos y sabe más de seguros, riesgos y pólizas que una compañía de seguros. Sin embargo, parece poco recomendable, por ejemplo, que dediquen sus esfuerzos a obtener un algoritmo capaz de conversar correctamente, porque sería equivalente a reinventar la rueda o a programarse su propia hoja de cálculo.

La recomendación es partir de algoritmos de automatización avanzada, de *machine learning*, que pueden cada vez más ser diseñados, entrenados y creados con herramientas sencillas al alcance de cualquier directivo y sin prácticamente necesidad de programar, lo que reduce **los problemas derivados de su integración posterior con el resto de los sistemas de la compañía.**

A partir de ahí, plantearse que las piezas basadas en conocimiento más específico y propio de la compañía deberán, seguramente, ser diseñadas internamente, mientras que las soluciones más genéricas, como la integración en la ofimática, es más probable que provengan de compañías especializadas en ese tipo de herramientas.

Lo que sí tengo claro, como lo tuve en su momento con internet, es que las compañías que no hagan ese trabajo de integración estratégica de la inteligencia artificial, habrán desaparecido dentro de no mucho tiempo. Como decía el CEO de Google hace algunos años: “nuestra ventaja competitiva será que nuestros algoritmos sean más inteligentes que los de nuestros competidores”. Así de importante es la cosa. **Es momento de ponerse las pilas, de investigar y de preguntar.**

******Enrique Dans es Profesor de Innovación en IE University.***

MÁS DE ENRIQUE DANS

- ¿Y qué si el dióxido de carbono sigue subiendo?
  15 mayo, 2024 - 01:43