Flash Note: DeepSeek Bajo Fuego ¿Revolución o Ilusión? Prohibiciones, Filtraciones y los Obstáculos que Frenan su Expansión Global

DeepSeek irrumpió en la inteligencia artificial con la ambición de desafiar a los gigantes occidentales, pero su avance choca con una serie de obstáculos: preocupaciones legítimas sobre privacidad y seguridad, acusaciones de apropiación tecnológica, y ahora las primeras restricciones de su uso por parte de algunos gobiernos. La expansión global de esta IA china, lejos de estar asegurada, se enfrenta a una incertidumbre que crece a cada día que pasa, transformando la promesa de una revolución en una posible ilusión pasajera. A continuación, los factores que, a mi juicio, podrían imponer un límite estricto al desarrollo de esta IA china.

Preocupaciones de Privacidad con DeepSeek

Expertos en ciberseguridad han expresado preocupaciones sobre la posibilidad de que DeepSeek esté transmitiendo información de los usuarios al gobierno chino. Investigaciones han revelado que el sitio web de DeepSeek contiene código que podría enviar datos de inicio de sesión de los usuarios a China Mobile, una empresa estatal de telecomunicaciones con vínculos militares. La política de privacidad de DeepSeek indica que los datos se almacenan en servidores chinos, lo que podría permitir la creación de "huellas digitales" para rastrear las actividades de los usuarios en otros sitios web.

La cadena bbc citó informes recientes que indican que la plataforma de IA generativa DeepSeek está transfiriendo una gran cantidad de datos de usuarios estadounidenses directamente a China. Esta revelación ha intensificado las preocupaciones sobre la privacidad y la seguridad de los datos, especialmente en medio de las tensiones tecnológicas entre Estados Unidos y China. *bbc.com*

Vulnerabilidades del propio modelo de DeepSeek

Pruebas recientes han revelado que el modelo más reciente de DeepSeek, R1, es más susceptible a ser manipulado que el modelo de competidores como ChatGPT de OpenAI y Gemini de Google. Estas vulnerabilidades permiten que DeepSeek sea inducido a proporcionar información peligrosa, como instrucciones que promueven el autodaño. Aunque la aplicación rechaza solicitudes directas de contenido dañino, sus salvaguardias pueden ser eludidas mediante métodos de manipulación complejas. Y es que la naturaleza de código abierto de DeepSeek permite modificaciones, lo que podría aumentar los riesgos asociados con el uso indebido de la IA. Estos hallazgos subrayan la necesidad crítica de priorizar las medidas de seguridad en el desarrollo de IA. De ahí la mayor opacidad en los proveedores americanos. *wsj.com*

Prohibiciones y Restricciones a DeepSeek

- **Corea del Sur, Taiwán y Australia prohíben el uso de DeepSeek:** Varios países han tomado medidas contra el uso de DeepSeek debido a preocupaciones de seguridad nacional y privacidad de datos. Corea del Sur, Taiwán y Australia han prohibido la aplicación en dispositivos gubernamentales, y se espera que más países sigan su ejemplo. En el caso de Australia, la decisión se tomó siguiendo una directiva del Departamento de Asuntos Internos de Australia que identificó a DeepSeek como un "riesgo significativo para la seguridad". Aunque la prohibición no se extiende al uso privado, se aconseja encarecidamente a los ciudadanos que eviten utilizar la aplicación debido a posibles riesgos de seguridad. No descarto que acabe extendiéndose a todo el ámbito privado. TPG Telecom en Australia ha prohibido a sus empleados utilizar DeepSeek, tanto en el trabajo como en su vida privada. *news.com.au*

- **Texas prohíbe DeepSeek por preocupaciones de seguridad:** El gobernador de Texas, Greg Abbott, ha anunciado la prohibición de la aplicación de IA DeepSeek en dispositivos emitidos por el gobierno estatal. La medida se basa en preocupaciones de seguridad relacionadas con la posible exposición de datos al Partido Comunista Chino.

- **DeepSeek, por su parte, se acerca a las startups europeas,** proporcionándoles la oportunidad de ponerse al día en la carrera global de IA al ofrecer precios significativamente más bajos en comparación con modelos estadounidenses como OpenAI.

DeepSeek. Un modelo replicable

Esfuerzos de código abierto liderados por Hugging Face están examinando las técnicas de DeepSeek para replicar el modelo en semanas, lo que podría inaugurar una nueva era de IA rentable,

Acusaciones de Uso Indebido de Tecnología por parte de DeepSeek

OpenAI ha acusado a DeepSeek de utilizar su tecnología sin autorización mediante un proceso conocido como "destilación". Este método implica bombardear un modelo de IA, como ChatGPT, con preguntas y utilizar las respuestas para entrenar un nuevo modelo. Eso explicaría porque DeepSeek ha desarrollado un modelo de IA de alto rendimiento a un costo mucho menor, lo que ha generado sospechas sobre el origen de su tecnología. Aunque la destilación no se considera piratería, viola los términos de servicio de OpenAI y plantea preocupaciones sobre la proliferación de modelos de IA no autorizados.

Colaboración entre Rusia y China en Investigación de IA

El presidente Putin ha instado a Sberbank a construir cooperación en IA con China. Dicho y hecho. Sberbank, el banco más grande de Rusia, ha anunciado planes para colaborar con investigadores chinos en proyectos conjuntos de inteligencia artificial tras el éxito de DeepSeek. Moscú busca fortalecer la cooperación en IA con China en medio de una asociación estratégica que ambas naciones consideran crucial frente a Occidente. No creo que esta "alianza" estratégica entre Rusia y China en el campo de la IA haga ningún bien a China, ya que la entrada de Rusia en esta alianza a buen seguro va a perturbar al sector global de IA. Por todos es conocida la intención de ambos países de contrarrestar la influencia de Estados Unidos, más si cabe cuando ambos países se sirven de la propia tecnología americana, mediante la práctica del "distillation" para intentar alcanzar a los proveedores americanos. No lo sé, pero todo esto me huele a una inminente limitación del uso de DeepSeek en el ámbito privado occidental. Sberbank también ha hecho que sus plataformas de IA sean accesibles públicamente, fomentando una gran comunidad, una estrategia que contrasta con el secretismo de sus contrapartes estadounidenses como OpenAI. Entiendo que esto puede pesar mucho en las decisiones del consumidor, y mantener la presión elevada para que las autoridades no decidan limitar el uso de la IA China en occidente.

Mientras, la integración de DeepSeek en Empresas Chinas continua.

Varias empresas chinas están adoptando la tecnología de inteligencia artificial de DeepSeek. Great Wall Motor ha integrado DeepSeek en su sistema de vehículos. Los principales proveedores de telecomunicaciones, como China Mobile, China Unicom y China Telecom, están colaborando con el modelo de código abierto de DeepSeek. Sin embargo, algunas empresas, como Capitalonline Data Service y MeiG Smart Technology, han advertido a los inversores que los beneficios comerciales derivados del modelo de DeepSeek aún son inciertos. *reuters.com*

Cordiales saludos

Alex Fuste
Chief Global Economist
ANDBANK