Úc cấm DeepSeek khỏi các thiết bị của chính phủ.

Nguồn: 'Australia bans DeepSeek from government devices: experts react' © The University of Sydney (6/2/25)

© Ảnh minh họa. © Wiki

Artificial intelligence (AI) platform DeepSeek has been banned on all federal government systems and devices in Australia, following security and privacy concerns. University of Sydney experts from the Faculty of Engineering and University of Sydney Business School weigh in regarding the impact of DeepSeek on technology, society, cybersecurity and industry.

Không kiểm soát được cách sử dụng dữ liệu Tiến sĩ Jonathan Kummerfeld từ Khoa Khoa học Máy tính thuộc Khoa Kỹ thuật cho biết đây là một động thái thận trọng vì hiện tại không có cách nào kiểm soát được cách dữ liệu được cung cấp cho chatbot được sử dụng. Tiến sĩ Kummerfeld làm việc về AI và xử lý ngôn ngữ tự nhiên, đặc biệt tập trung vào các hệ thống cộng tác giữa con người và các mô hình AI

"Đồng thời, điều quan trọng cần lưu ý là Úc có thể hưởng lợi từ những khám phá khoa học hỗ trợ DeepSeek. Chúng ta có thể sử dụng những sáng kiến đó để xây dựng hệ thống của riêng mình mà không phải chịu rủi ro khi sử dụng dịch vụ chatbot", Tiến sĩ Kummerfeld cho biết.

DeepSeek là mã nguồn mở đặt ra thách thức độc đáo

Tiến sĩ Suranga Seneviratne, chuyên gia về quyền riêng tư và an ninh mạng, cho biết tương tự như trường hợp của TikTok, quyết định này không có gì đáng ngạc nhiên khi xét đến những rủi ro tiềm ẩn.

"Các mô hình ngôn ngữ lớn (LLM) đưa ra những mối quan tâm nổi tiếng, bao gồm quyền riêng tư dữ liệu, tính bảo mật và khả năng chứa các cửa hậu. Ngoài ra, mặc dù có những tiến bộ đáng kể gần đây, LLM vẫn có thể gây ảo giác, nghĩa là đầu ra của chúng phải được xác minh trong các cài đặt quan trọng.

"Ngoài bản thân AI, việc ứng dụng truy cập vào dữ liệu người dùng—chẳng hạn như clipboard—có thể gây ra thêm rủi ro. Một thách thức độc đáo phát sinh từ việc DeepSeek là mã nguồn mở; trong khi công ty ban đầu kiểm soát các phiên bản web và ứng dụng chính thức, bất kỳ ai cũng có thể lưu trữ phiên bản của riêng họ. Điều này khiến lệnh cấm hoàn toàn trở nên khó thực thi, mặc dù trong trường hợp này, rủi ro có thể được coi là thấp", Tiến sĩ Seneviratne, từ Khoa Khoa học Máy tính, Khoa Kỹ thuật cho biết.

"Mọi người hiện nay có xu hướng tin tưởng mù quáng vào nội dung do AI tạo ra. AI có thể cố ý hoặc vô tình tạo ra ảo giác hoặc đưa ra câu trả lời sai, nhưng mọi người vẫn

tin tưởng nó như thể nó đến từ các nguồn đáng tin cậy," Tiến sĩ Armin Chitizadeh, Khoa Khoa học máy tính, Khoa Kỹ thuật.

Người sử dụng cần thận trọng hơn với các công cụ AI

Tiến sĩ Armin Chitizadeh, chuyên gia về đạo đức AI tại Khoa Khoa học Máy tính, Khoa Kỹ thuật cho biết mọi người cần thận trọng hơn khi sử dụng bất kỳ công cụ GenAI nào.

"Sự xuất hiện của các công cụ GenAI đã gây ra nhiều vấn đề và tôi rất vui vì sự xuất hiện của DeepSeek đã tạo nên làn sóng lo ngại.

"Mối lo ngại đầu tiên là trong cuộc đua tạo ra AI nhanh nhất và tốt nhất, các công ty có thể cắt giảm cách lưu trữ dữ liệu khách hàng, không dành đủ thời gian để bảo vệ dữ liệu khỏi các tác nhân độc hại.

"Mối quan ngại thứ hai là mọi người hiện có xu hướng tin tưởng mù quáng vào nội dung do AI tạo ra. AI có thể cố ý hoặc vô tình tạo ra ảo giác hoặc đưa ra câu trả lời sai, nhưng mọi người vẫn tin tưởng như thể nó đến từ các nguồn đáng tin cậy.

"Mối quan tâm thứ ba và có thể là quan trọng nhất là AI có thể dễ dàng lý luận và rút ra những kết luận quan trọng từ dữ liệu người dùng có vẻ không đáng kể. Người dùng có thể cung cấp dữ liệu cho các công cụ GenAI, cho rằng dữ liệu đó không có giá trị. Tuy nhiên, AI có thể kết nối các điểm và đưa ra những kết luận quan trọng. Thông tin mới suy ra này sau đó nằm trong tay chủ sở hữu công cụ GenAI, người có toàn quyền kiểm soát việc sử dụng và bán dữ liệu đó."

Giáo sư Kai Reimer, Trường Kinh doanh Đại học Sydney và Giám đốc Sydney Executive Plus, *"Bất kể là Trung Quốc hay bất kỳ quốc gia nào khác: dữ liệu của chính phủ không nên được lưu trữ ở nước ngoài và bên ngoài các hệ thống an toàn của Úc."*

Tác động đến ngành công nghiệp AI là câu chuyện có thật

Giáo sư Kai Riemer là Giáo sư Công nghệ thông tin và Tổ chức tại Trường Kinh doanh thuộc Đại học Sydney và là Giám đốc của Sydney Executive Plus, nơi ông giảng dạy khóa đào tạo quản lý cấp cao về khả năng sử dụng AI thành thạo.

"Điều này tạo ra nhiều sự quan tâm vì đó là AI và Trung Quốc, nhưng đó chỉ là bảo mật dữ liệu thận trọng. Không quan trọng là Trung Quốc hay bất kỳ quốc gia nào khác: dữ liệu của chính phủ không nên được lưu trữ ở nước ngoài và bên ngoài các hệ thống an toàn của Úc", Giáo sư Reimer cho biết.

"Câu chuyện thực sự ở đây là cách các nền tảng nguồn mở này dường như đang đảo ngược kỹ thuật đột phá của những người tiên phong như OpenAI và tác động đến mô hình kinh doanh của ngành AI. Tôi ví các sản phẩm như DeepSeek và Meta AI với MP3: chúng không phát minh ra nhạc được ghi âm, nhưng kỹ thuật nén thông minh này đã có tác động rất lớn đến cách chúng ta truy cập nhạc."

Cấm là một biện pháp phòng ngừa để bảo vệ an ninh quốc gia (Ban a pre-emptive measure to protect national security)

Giáo sư Uri Gal là Giáo sư Hệ thống thông tin kinh doanh tại Trường Kinh doanh Đại học Sydney. Nghiên cứu của ông tập trung vào các khía cạnh tổ chức và đạo đức của công nghệ số, bao gồm bảo mật dữ liệu.

"Các cơ quan chính phủ thường quản lý thông tin cực kỳ nhạy cảm và có lo ngại rằng việc thu thập dữ liệu rộng rãi của DeepSeek - chẳng hạn như thông tin chi tiết về thiết bị, số liệu sử dụng và mã định danh cá nhân - có thể khiến thông tin bí mật dễ bị tấn công nếu bị truy cập hoặc lưu trữ bên ngoài biên giới Úc. Mặc dù bản chất mã nguồn mở của mô hình này mang lại sự minh bạch về mã của nó, nhưng nó không đảm bảo rằng dữ liệu người dùng chỉ được xử lý trong phạm vi Úc hoặc theo các tiêu chuẩn bảo mật của địa phương. Rủi ro truy cập dữ liệu xuyên biên giới này là một yếu tố chính đằng sau lệnh cấm.

"Ngoài các ứng dụng của chính phủ, AI tạo ra như DeepSeek còn gây ra thêm nhiều rủi ro cho công chúng. Những rủi ro này bao gồm khả năng phát tán thông tin sai lệch, sự thiên vị không chủ ý trong kết quả và rủi ro vi phạm quyền riêng tư nếu dữ liệu cá nhân vô tình bị tiết lộ hoặc sử dụng sai mục đích.

"Hơn nữa, quy mô và tính tự động hóa của các hệ thống như vậy có thể dẫn đến những thách thức về trách nhiệm giải trình, có thể làm phức tạp thêm các nỗ lực truy tìm và sửa chữa nội dung sai lệch hoặc có hại. Do đó, lệnh cấm có thể được coi là một biện pháp phòng ngừa nhằm bảo vệ an ninh quốc gia và niềm tin của công chúng cho đến khi các biện pháp bảo vệ dữ liệu mạnh mẽ được thiết lập."

Related Subjects:

- Lệnh cấm DeepSeek của Trung Quốc trên tất cả các thiết bị của chính phủ Úc, được đưa ra chỉ vài ngày sau khi một công ty an ninh mạng của Úc cảnh báo rằng dữ liệu đầu ra của DeepSeek và dữ liệu người dùng mà công ty này thu thập - *"gần như chắc chắn… chịu sự chỉ đạo và kiểm soát của chính phủ Trung Quốc".*

- 'Hành động nhanh và phá vỡ mọi thứ': Dự án AI trị giá 500 tỷ đô la của Trump có rủi ro lớn! Dự án Stargate, nhằm mục đích đẩy nhanh việc ứng dụng AI tại Hoa Kỳ – nhưng điều này cũng đi kèm với những rủi ro riêng. Nếu chúng ta so sánh hệ thống AI với một chiếc ô tô, điều này giống như việc phát triển một chiếc ô tô nhanh nhất có thể trong khi bỏ qua các tính năng an toàn quan trọng như dây an toàn hoặc túi khí để làm cho nó nhẹ hơn và chạy nhanh hơn! (TS Amin Chitizadeh Sydney Uni, 23/1/25).

- Trump highlights partnership investing $500 billion in AI