E-Bezpečí 2025, 10(1): Page 5-7. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4392

ČÍNSKÁ UMĚLÁ INTELIGENCE DEEPSEEK: REVOLUCE S OTAZNÍKY A HROZBOU PRO SOUKROMÍ

Kamil KOPECKÝ

Čínský startup DeepSeek způsobil na přelomu roku 2025 pozdvižení v technologickém světě. Jeho AI model se stal nejstahovanější aplikací v USA a výrazně ovlivnil hodnotu akcií amerických technologických gigantů. Přestože DeepSeek přináší inovace a úspornost, vyvolává také vážné otázky ohledně bezpečnosti dat, možného zneužití čínskou vládou a etiky vývoje.

DeepSeek je **čínský model umělé inteligence (AI), který funguje podobně jako známé chatboty ChatGPT od OpenAI nebo Gemini od Googlu**. Jedná se o pokročilý systém strojového učení, který dokáže odpovídat na otázky, generovat texty, analyzovat data a vést konverzace s uživateli. Hlavní rozdíl spočívá v tom, že DeepSeek pochází z Číny, a proto podléhá tamním zákonům a regulacím, což může ovlivnit způsob, jakým pracuje s informacemi a osobními daty uživatelů.

DeepSeek tvrdí, že dokázal vytvořit špičkovou umělou inteligenci s rozpočtem pouhých 5,6 milionu dolarů, zatímco konkurenti jako OpenAI investovali do vývoje stovky milionů. Díky efektivitě a dostupnosti se DeepSeek rychle rozšířil po celém světě, což vedlo k rekordnímu propadu akcií amerických společností. Nvidia zaznamenala jednodenní ztrátu téměř 600 miliard dolarů, podobně dopadl Alphabet (Google) i Microsoft.

Čínská vláda vidí v DeepSeek nástroj pro globální technologickou dominanci a ukazuje, že je schopna konkurovat americkým

gigantům i s minimálními náklady.

DeepSeek není jen technologickým průlomem, ale také **nástrojem cenzury**. Na citlivé otázky, jako jsou protesty na náměstí Nebeského klidu, status Tchaj-wanu nebo čínská lidskoprávní politika, model odmítá odpovědět nebo nabízí odpovědi v souladu s oficiální čínskou propagandou. Tento přístup vzbuzuje obavy o manipulaci informací a omezování svobody slova.

Největší obavy vzbuzuje způsob, jakým DeepSeek nakládá s uživatelskými daty. **Podmínky užívání služby umožňují přístup ke konverzacím uživatelů a jejich analýzu. Navíc tato data mohou být sdílena s „partnery společnosti“, což v čínském právním kontextu zahrnuje i státní úřady**. Čínská legislativa, zejména zákon o kybernetické bezpečnosti a zákon o ochraně osobních údajů, umožňuje čínské vládě přístup k datům z jakékoli domácí technologické firmy. To znamená, že jakákoli komunikace vedená přes DeepSeek – ať už osobní, obchodní či politická – může být v konečném důsledku využita čínskou stranou.

Objevila se také podezření, že DeepSeek mohl při vývoji svých modelů využít data z OpenAI. Podle některých zpráv existují náznaky, že DeepSeek mohl použít techniky tzv. "destilace" modelů k získání znalostí z modelů OpenAI, což by mohlo představovat porušení etických standardů ve vývoji AI.

Co hrozí uživatelům?

Sledování a profilování – Čínská vláda má možnost analyzovat chování uživatelů, identifikovat jejich politické názory či ekonomické strategie.
Průmyslová špionáž – DeepSeek může shromažďovat citlivé informace od firem a institucí, které jej využívají, a tyto informace mohou být využity ve prospěch čínského průmyslu.
Cenzurování a manipulace – Systém může cíleně potlačovat informace nebo nabízet zkreslené odpovědi, což může ovlivňovat veřejné mínění.

V USA i Evropě se již diskutuje o regulaci DeepSeek a možném

zákazu jeho používání v citlivých oblastech, podobně jako tomu bylo u čínské aplikace TikTok. Americký prezident Donald Trump označil situaci za „budíček“ a vyzval k podpoře domácího AI průmyslu.

Odborníci varují, že pokud bude DeepSeek i nadále expandovat, mohl by se stát jedním z největších globálních sběračů dat s nejasnými dopady na geopolitiku i kybernetickou bezpečnost.

Redakce E-Bezpečí

Zdroje:

Seznam Zprávy
iROZHLAS
CNN Prima News
Česká televize
Hospodářské noviny
The Verge