Korea Południowa blokuje DeepSeek na komputerach rządowych z powodu obaw o szpiegostwo

Południowokoreańska Narodowa Służba Wywiadowcza (NIS) zaleciła agencjom rządowym zablokowanie dostępu do DeepSeek, chińskiego chatbota sztucznej inteligencji (AI), ze względu na obawy dotyczące nadmiernego gromadzenia danych i potencjalnego chińskiego szpiegostwa.

Posunięcie, które weszło w życie w tym tygodniu, jest następstwem biuletynu bezpieczeństwa wydanego przez NIS, który szczegółowo opisywał praktyki DeepSeek, w tym przechowywanie danych użytkowników na chińskich serwerach i udzielanie stronniczych odpowiedzi na wrażliwe pytania.

Decyzja o zablokowaniu DeepSeek pojawia się w czasie, gdy Korea Południowa, wraz z innymi krajami, takimi jak Australia, Tajwan i Włochy, coraz bardziej obawia się zagrożeń bezpieczeństwa stwarzanych przez chińską technologię. NIS ostrzegł, że praktyki DeepSeek w zakresie danych mogą ujawnić poufne informacje rządowe chińskiemu rządowi, który ma prawo dostępu do danych przechowywanych w jego granicach.

Nadmierne gromadzenie danych i tendencyjne odpowiedzi

Według NIS metody gromadzenia danych przez DeepSeek są bardziej inwazyjne niż w przypadku innych usług AI. Agencja stwierdziła, że DeepSeek „zawiera funkcję zbierania wzorców wprowadzania danych z klawiatury, które mogą identyfikować osoby i komunikować się z serwerami chińskich firm, takimi jak volceapplog.com”. Możliwości te, w połączeniu z warunkami korzystania z aplikacji, które pozwalają na przechowywanie danych przez czas nieokreślony i nieograniczony dostęp do nich przez zewnętrznych reklamodawców, wzbudziły poważne obawy dotyczące prywatności.

Jednym z najbardziej niepokojących aspektów zachowania DeepSeek są tendencyjne odpowiedzi na pytania dotyczące wrażliwych tematów. Na przykład na pytanie o pochodzenie kimchi, tradycyjnej koreańskiej potrawy, DeepSeek udzielił różnych odpowiedzi w zależności od języka zapytania. W języku koreańskim uznała kimchi za danie koreańskie, ale gdy zapytano ją po chińsku, twierdziła, że danie pochodzi z Chin. Ta rozbieżność nie jest odosobniona; NIS zauważył również, że odpowiedzi DeepSeek na pytania dotyczące Projektu Północno-Wschodniego, chińskiej inicjatywy badawczej, która twierdzi, że starożytne królestwa koreańskie są terytorium Chin, były pod silnym wpływem propagandy Komunistycznej Partii Chin (KPCh).

Globalne obawy i ograniczenia

Korea Południowa nie jest osamotniona w swoich obawach. Australia i Tajwan również zakazały DeepSeek na urządzeniach rządowych, powołując się na zagrożenia dla bezpieczeństwa narodowego. Włoski organ nadzorujący prywatność nakazał ogólnokrajową blokadę DeepSeek, dając firmie 20 dni na wyjaśnienie, w jaki sposób przestrzega europejskich przepisów

o ochronie danych. Stany Zjednoczone, w tym agencje takie jak NASA i US Navy, również ograniczyły korzystanie z DeepSeek ze względu na obawy dotyczące bezpieczeństwa i prywatności.

Działania te odzwierciedlają rosnący globalny trend ostrożności wobec chińskiej technologii sztucznej inteligencji. Stany Zjednoczone nałożyły ścisłe kontrole eksportu zaawansowanych chipów i sprzętu do produkcji chipów do Chin, mając na celu ograniczenie rozwoju sztucznej inteligencji. Jednak pojawienie się DeepSeek jako taniej i wydajnej alternatywy dla amerykańskich modeli sztucznej inteligencji zachwiało zaufaniem inwestorów i wywołało pytania o przyszłość globalnej konkurencji w dziedzinie sztucznej inteligencji.

Decyzja o zablokowaniu DeepSeek na komputerach rządowych Korei Południowej podkreśla zaangażowanie tego kraju w ochronę danych swoich obywateli i bezpieczeństwa narodowego. W miarę jak inne kraje idą w ich ślady, społeczność międzynarodowa wysyła Chinom jasny komunikat: globalny krajobraz sztucznej inteligencji nie zostanie zdominowany przez technologię, która narusza prywatność i suwerenność. Rozwój DeepSeek nie tylko wywołał technologiczny wyścig zbrojeń, ale także nasilił napięcia geopolityczne między Wschodem a Zachodem.