R1: zagrożenie czy szansa dla europejskiego rynku?

Ewa Dolińska-Wysocka
radczyni prawna, członkini Sekcji Aktualne Wyzwania Sztucznej Inteligencji Polskiego Towarzystwa Informatycznego, ekspertka Grupy Roboczej ds. Sztucznej Inteligencji przy Ministrze Cyfryzacji.

Zdecydowana większość formułowanych wobec DeepSeek zastrzeżeń i zakazów związanych z przetwarzaniem danych dotyczy korzystania z modelu przez aplikację mobilną, interfejs czy API udostępniane bezpośrednio przez DeepSeek, a nie lokalnie czy przez platformy firm trzecich posiadające wyższy poziom zabezpieczeń i dostosowane do standardów polityki prywatności UE.

Parametry, w tym wagi, informacje na temat architektury oraz korzystania z modelu DeepSeek, zostały upublicznione. Oznacza to, że DeepSeek R1 ma szansę skorzystać z wyłączeń regulacyjnych przewidzianych przez AI Act (AIA) dla modeli open source ogólnego przeznaczenia[1]. Pod jednym warunkiem, że nie zostanie zaklasyfikowany jako model stwarzający ryzyko systemowe.

Co prawda rozmiar R1 jest znacznie poniżej progu 10^{25} FLOPs określonego w AIA, nie można jednak wykluczyć, że ze względu na lawinowo rosnącą liczbę użytkowników zostanie on w przyszłości wyznaczony jako model stwarzający ryzyko systemowe, mimo że znajduje się on znacznie poniżej wspomnianego progu. W takim przypadku DeepSeek nie mógłby skorzystać z wyłączeń przewidzianych dla modeli open source, ponieważ nie mają one zastosowania do modeli obarczonych ryzykiem systemowym. Jeśli tak się stanie, DeepSeek zobowiązany będzie do podjęcia działań służących ocenie i ograniczeniu tego ryzyka pod rygorem kary grzywny, a nawet ograniczenia dostępu do jednolitego rynku unijnego.

Nie ma jednak pewności, że DeepSeek dostosuje się do wymogów AIA. Na razie chińska firma twierdzi, że nie działa w Europie i nie mają do niej zastosowania europejskie regulacje[2].

Czy szansą dla europejskich firm pozostaje jedynie zapowiadana deregulacja? Odpowiedź na to pytanie w dużej mierze zależy od wytycznych, jakie zostaną włączone do opracowywanego aktualnie kodeksu postępowania w zakresie sztucznej inteligencji do celów ogólnych (Code of Practice for General-Purpose AI)[3].

Ponieważ modele sztucznej inteligencji ogólnego przeznaczenia mogą być dalej modyfikowane lub dostosowywane, pojawia się wątpliwość, czy taki zmieniony model stanowi model odrębny od modelu bazowego i w jakim zakresie dostawca zmienionego modelu powinien odpowiadać za „odziedziczone" po modelu bazowym wady. W przypadku DeepSeek pytanie to wydaje się szczególnie istotne ze względu na zarzuty stawiane Chińczykom

1 Motyw 102 preambuły AIA wskazuje, że aby model sztucznej inteligencji mógł być uznany za oprogramowanie opensource, musi być on udostępniony na licencji otwartego oprogramowania, która umożliwia jego ogólne upowszechnianie i zezwala użytkownikom na swobodny dostęp do nich, ich wykorzystywanie, zmianę i ich redystrybucję lub ich zmienionych wersji.

2 Źródło: https://garanteprivacy.it/home/docweb/-/docweb-display/docweb/10097450#english

3 Więcej o kodeksie: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice/

przez OpenAI dotyczące rzekomego stosowania techniki „destylacji" poprzez wykorzystanie modeli OpenAI do trenowania DeepSeek[4], co naruszałoby warunki korzystania z usług OpenAI, a dodatkowo mogłoby stanowić czyn nieuczciwej konkurencji. Dla równowagi trzeba jednak dodać, że podobne oskarżenia wysuwane były w 2023 r. pod adresem Google'a w związku z udostępnianym przez tę firmę modelem Bard.

Aktualne stanowisko Europejskiego Urzędu ds. Sztucznej Inteligencji jest takie, że w przypadku modyfikacji lub dopracowania istniejącego modelu sztucznej inteligencji ogólnego przeznaczenia obowiązki dostawców, także dostawców modeli obarczonych ryzykiem systemowym, powinny ograniczać się jedynie do części przez nich zmodyfikowanej lub dopracowanej (np. uzupełnienia dokumentacji w tym zakresie[5]). Ogólny kodeks postępowania w zakresie sztucznej inteligencji ma szansę odnieść się do tej kwestii.

Jeżeli finalnie zostałoby ustalone, że dotrenowanie i inne techniki szkoleniowe są jedynie formą dopracowania modelu, wówczas dostawca rozwiązania bazującego na dotrenowanym R1 musiałby jedynie udokumentować część rozwiązania odpowiadającą dodanej przez niego wartości. Pozwoliłoby to w szczególności na uniknięcie konieczności analizy, czy i w jakim stopniu zarzuty OpenAI wobec DeepSeek są prawdziwe, a potencjalnie również – „dziedziczenia" ryzyka systemowego.

Otworzyłoby to drogę europejskim startupom do konkurowania z dużymi firmami technologicznymi, które oferują produkty bazujące na własnych komercyjnych modelach. Ten scenariusz dobrze wpisuje się w zauważalną ostatnio w Unii Europejskiej potrzebę poprawy pozycji Europy w „wyścigu o sztuczną inteligencję" i pozwoliłby wypełnić lukę na rynku związaną z niechęcią amerykańskich dostawców do dostosowania wszystkich swoich produktów opartych na AI do nowych wymogów unijnych.

---

4 Więcej: https://www.ft.com/content/a0dfedd1-5255-4fa9-8ccc-1fe01de87ea6?accessToken=zwAGLNJX-fBAkdOg3-3RUlVPqdOMzB_gHeh-pg.MEYCIQCGjo04z0mtOsKbDspQLq2BMXyw8SbQnlYePOuqiqr6QgIhAInK67eBkYuZS-77ljnP-y--EJdN1wwRQ8GIR8sKMFgE&sharetype=gift&token=1eebbaa7-a4e6-4251-b665-c2f2562b38e4 (dostęp aktywny na dzień 20 lutego 2025 r.). Dodatkowo społeczność OpenAI podaje, że wcześniejsze wersje DeepSeek identyfikowały się jako ChatGPT lub GPT-4, co sugeruje, że dane treningowe mogły pochodzić z modeli OpenAI – https://community.openai.com/t/is-deepseek-a-distilled-version-of-gpt-4-analyzing-suspicious-behavior/1109600.

5 Źródło: https://digital-strategy.ec.europa.eu/pl/faqs/general-purpose-ai-models-ai-act-questions-answers

Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego '25

ZASTOSOWANIA SZTUCZNEJ INTELIGENCJI

Szczegóły wkrótce na stronie www.sdsi.pl

PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

SEP

NOT