econopoly.ilsole24ore.com

DeepSeek tra innovazione, tutela della privacy e cyber-rischi

Numeri idee progetti per il futuro

Post di Ivan Ranza, CEO di ***Epicode*** *–*

Il lancio di DeepSeek-r1 ha stravolto le logiche dei modelli linguistici di grandi dimensioni (LLM), scardinando una delle teorie cardine secondo cui il successo di questi sistemi dipende dalla quantità di risorse computazionali e dalla dimensione del training del modello.

Un fattore chiave della rapida ascesa dell'app cinese (che non è più disponibile negli appstore Apple e Google mentre quest post viene pubblicato, ndr), costata oltretutto molto meno rispetto alle controparti americane, è stato il modello di business *freemium*, oltre all'architettura *open source* che consente agli utenti di eseguire il sistema su server privati, evitando così i costi richiesti da aziende come OpenAI e aumentando il controllo degli utenti stessi sulle risorse utilizzate.

Il successo di DeepSeek è stato tale da superare la popolarità di ChatGPT in un tempo irrisorio, cosa che ha riacceso prepotentemente il faro sulla sicurezza di questi sistemi e sulla consapevolezza degli utenti finali dei rischi ad essi correlati. Ad alimentare la fiamma si è aggiunta poi la dichiarazione della società, che ha annunciato di aver limitato le nuove registrazioni alla piattaforma a causa dell'elevato numero di attacchi malevoli ai suoi servizi, pur non specificandone l'origine.

Potenziale rivoluzionario, ma cybersicurezza prima priorità

I timori sono reali, perché ci possono essere delle conseguenze legate all'integrazione dell'AI nella nostra vita quotidiana. Queste esistono indipendentemente da chi fornisce la tecnologia, ma è comprensibile la ripercussione che questa sequela di notizie ha avuto sui mercati e, in particolare, sui produttori di chip, che vedono barcollare le basi della loro leadership.

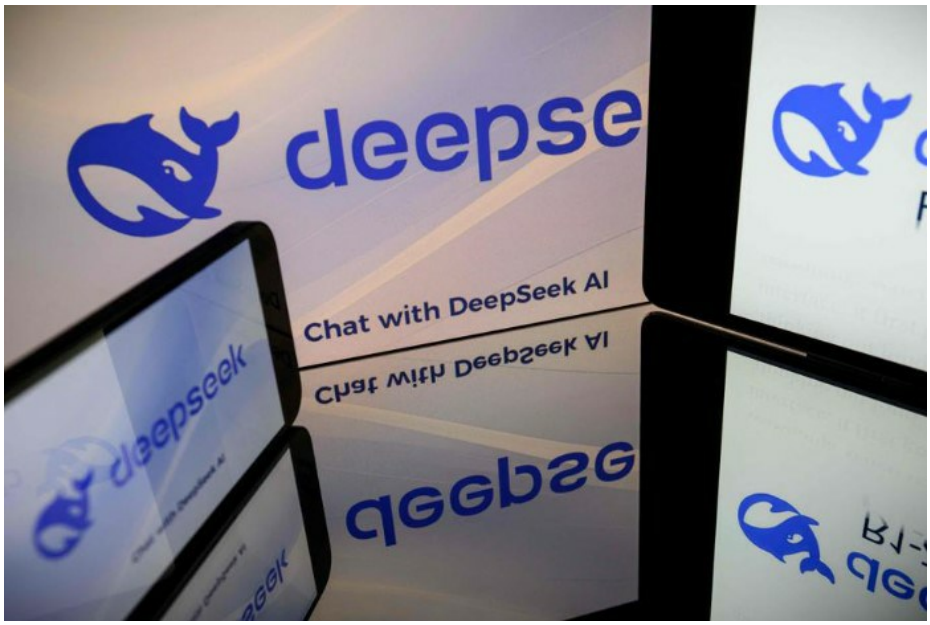
L'AI ha il potenziale di influenzare tutto, dalla sicurezza dei dati personali alle strategie di difesa nazionale, cosa che ha portato già da tempo la questione della cybersicurezza in cima alle priorità. Questo significa che c'è un dibattito su come rendere questa tecnologia più sicura, non che ci siano dubbi sul suo potenziale rivoluzionario.

Occorre essere utenti oculati: nonostante molte piattaforme LLM rassicurino gli utenti, è evidente che condividere informazioni sensibili della propria azienda o della propria vita personale non sia un'idea ottimale. Elaborare un documento finanziario tramite l'AI per

riceverne una sintesi, ad esempio, è comodo, ma può esporre a rischi significativi.

Se non paghi il prodotto sei sempre tu. DeepSeek cerca dati

In questo senso, è bene ricordare il messaggio reso popolare da *The Social Dilemma*, documentario Netflix di Jeff Orlowski: “Se non paghi il prodotto, il prodotto sei tu”. Uno degli esempi più recenti è il caso di Pokémon Go, promosso da Niantic, il cui uso gratuito è stato funzionale per l’azienda per raccogliere le scansioni del mondo degli utenti per costruire un modello che aiuterà i robot a navigare nello spazio fisico.



Schermi con il logo di DeepSeek. (Foto di Lionel BONAVENTURE / AFP)

In questo contesto, possiamo fare una duplice riflessione. Da un lato, la gratuità di DeepSeek potrebbe nascondere un obiettivo simile, ovvero la ricerca di nuovi dati. Dall’altro, il suo modello, come quello di Llama, eseguito in *self-hosting*, ovvero ospitato su server aziendali, permette di mantenere le informazioni all’interno della rete aziendale; così si evita che dati sensibili possano uscire dal perimetro di controllo, riducendo i rischi legati alla protezione della privacy.

Se l’innovazione corre più delle tutele

Una cosa possiamo dare per certa: l’ascesa di DeepSeek deve servire da monito sulla necessità di una maggiore consapevolezza di tutti gli attori coinvolti in tema di sicurezza, in un mondo dove l’innovazione potrebbe procedere più velocemente della capacità di tutelare chi la utilizza.

Tutto ciò che facciamo, preferiamo, cerchiamo sul digitale costituisce un dato che potrebbe

essere usato in modi che forse non possiamo ancora comprendere. Ci sarà, quindi, sempre maggiore bisogno di esperti in sicurezza informatica, sia a livello istituzionale sia a livello aziendale, a riprova che si rende necessario, mai come oggi, essere in grado di dare la giusta formazione alla nuova generazione di professionisti. Non una generazione anagrafica, ma scandita dalle competenze, tecniche e relazionali, che permettano loro di essere subito attive e operative sul campo.