

Tecno - *Dagli assistenti agli agenti: l'ascesa dell'IA agentica che pianifica e agisce in autonomia*

Roma - 07 apr 2026 (Prima Notizia 24) **Entro il 2030 gli "agenti" rappresenteranno il 31% del mercato dell'intelligenza artificiale generativa. Non più solo chatbot, ma sistemi capaci di navigare sul web, gestire bilanci e utilizzare software, portando però nuove sfide per la sicurezza informatica e la conformità europea.**

L'intelligenza artificiale sta compiendo il salto evolutivo definitivo: dal supporto puramente conversazionale alla capacità di azione autonoma. È l'era della "Agentic AI", una tecnologia che non si limita a creare testi o immagini, ma pianifica ed esegue compiti complessi interfacciandosi con strumenti esterni. Secondo le stime della società di analisi Omdia, questo segmento è destinato a dominare il settore, arrivando a coprire quasi un terzo dell'intero mercato dell'IA generativa entro il 2030, con tassi di crescita annuali del 175%. Il fenomeno ha subito un'accelerazione improvvisa grazie a progetti come OpenClaw (precedentemente noto come Clawdbot), il cui creatore Peter Steinberger è stato recentemente reclutato da OpenAI, confermando l'interesse dei giganti della Silicon Valley per gli agenti personali installabili localmente. I principali player tecnologici hanno già iniziato a integrare queste capacità nei propri ecosistemi. Se OpenAI ha sviluppato "Agent" per gestire attività trasversali, Google sta puntando su Gemini come un intermediario attivo capace di muoversi tra mappe, motori di ricerca e posta elettronica. Microsoft, attraverso Copilot Studio, permette invece alle aziende di creare agenti specializzati per l'analisi delle spese o la gestione del personale, mentre nuove realtà come Perplexity hanno lanciato sistemi progettati per navigare nel web e programmare flussi di lavoro in totale autonomia. L'adozione è massiccia: un rapporto di PwC rivela che l'88% dei dirigenti aziendali ha pianificato un aumento dei budget per implementare soluzioni agentiche, con il 79% delle organizzazioni che ha già avviato processi di integrazione. Tuttavia, questa capacità di "agire" solleva allarmi critici sul fronte della cybersicurezza e della normativa. L'IA agentica opera spesso in ambiti sensibili che l'AI Act europeo classifica "ad alto rischio". L'Enisa, l'agenzia dell'Ue per la cybersicurezza, ha inserito l'automazione guidata dall'IA tra le principali minacce per le infrastrutture critiche, segnalando il passaggio ad attacchi informatici sempre più dinamici e rapidi. I dati di CrowdStrike confermano questa urgenza: grazie all'automazione, il tempo necessario a un hacker per compromettere un sistema è sceso drasticamente da 48 a soli 29 minuti nell'ultimo anno. La sfida del prossimo futuro sarà dunque bilanciare l'incredibile efficienza operativa di questi agenti con la necessità di proteggere i dati e le infrastrutture da una minaccia che corre alla stessa velocità dell'innovazione.

(Prima Notizia 24) Martedì 07 Aprile 2026