Capgemini press contacts
Tiziana Sforza
Marketing & Communication
tiziana.sforza@capgemini.com
+39 348 7018984

TechnoVision: le cinque principali tendenze tecnologiche da tenere d'occhio nel 2027

Milano, 17 novembre 2026 – Capgemini ha presentato oggi *TechnoVision: Top 5 Tech Trends to Watch in 2027*, il report che individua le tecnologie che si prevede raggiungeranno un punto di svolta nel corso del prossimo anno. Mentre le aziende puntano a rendere sempre più autonomi i propri processi e le proprie attività operative, l'AI si apre a una nuova fase evolutiva, superando il ruolo di semplice «assistente» per trasformarsi in un sistema capace di agire ed eseguire attività in autonomia. Nel 2027, questa trasformazione è destinata a ridefinire i processi operativi aziendali, la cybersecurity, l'R&D e il commercio, aprendo nuove opportunità ma ponendo al contempo nuove sfide in termini di governance, sicurezza e resilienza.

"Lo scorso anno, le cinque principali tendenze tecnologiche individuate da Capgemini nel report Top 5 Tech Trends hanno evidenziato come l'AI stesse diventando sempre più integrata nell'architettura aziendale, nell'ingegneria del software e nei processi operativi delle imprese", spiega **Francesco Fantazzini**, **Chief Technology Innovation Officer di Capgemini in Italia**. *"Con gli agenti AI che operano in autonomia, questa tecnologia sta raggiungendo un punto di svolta. Guardando al 2027, la sfida principale per le aziende sarà riuscire a estendere l'autonomia senza perdere il controllo. Sarà quindi necessario gestire le interazioni tra gli agenti, contenere gli esiti imprevisti e rispondere alle minacce alla stessa velocità delle macchine. Al di là di queste sfide, l'AI agentica è destinata a trasformare i modelli di lavoro consolidati: dall'accelerazione dell'innovazione nella ricerca e sviluppo alla ridefinizione delle interazioni tra aziende e consumatori".*

Le tecnologie da tenere d'occhio nel 2027

1) L'azienda nell'era dell'AI agentica – sistemi multi-agente: interazioni autonome e imprevedibili tra agenti AI

Oggi, la maggior parte degli agenti AI e dei sistemi agentici è sufficientemente semplice da poter essere testata prima della sua messa in funzione. Tuttavia, con l'aumentare del loro numero, diventa impossibile verificare tutte le possibili interazioni. Per esempio, un'azienda che utilizza 15 agenti AI deve considerare 105 possibili interazioni a coppie; con 1.000 agenti e 200 sistemi agentici, il numero sale a quasi 720.000. Con un numero così elevato di agenti e sistemi, gli agenti possono generare comportamenti che non erano stati previsti in fase di progettazione. Ogni agente può prendere decisioni ragionevoli sulla base del proprio obiettivo e delle informazioni a disposizione; tuttavia, tali decisioni possono interagire tra loro, innescare reazioni da parte di altri agenti e, in ultima analisi, produrre conseguenze impreviste a livello di sistema. Ogni agente può agire correttamente, ma il sistema nel suo complesso può comunque fallire, con conseguenze potenzialmente gravi per l'azienda.

***Perché è importante*:** in futuro, il controllo dovrà articolarsi su tre livelli: un sistema di protezione e controllo per ciascun agente, un piano di controllo per ogni sistema agentico e un piano di controllo aziendale che li comprenda tutti. Nel 2027, i piani di controllo a livello aziendale dovranno includere un registro di tutti gli agenti e dei sistemi agentici, con le rispettive identità e autorizzazioni, il monitoraggio dei risultati prodotti e delle risorse utilizzate, la visibilità sulle interazioni tra gli agenti, limiti alle azioni che possono svolgere congiuntamente e la possibilità di arrestarli.

2) Autonomia affidabile e sicurezza dell'AI: dalla spiegabilità al contenimento dei rischi

Tradizionalmente, per garantire la sicurezza dei sistemi di AI si è fatto ricorso alla registrazione dei processi decisionali dell'intelligenza artificiale, alla limitazione degli accessi degli agenti e dei sistemi agentici e alla verifica che ogni decisione rispettasse le regole aziendali. Questo approccio, tuttavia, è sempre più difficile da applicare, poiché alcuni dei nuovi modelli non rendono più visibili tutti i passaggi del proprio ragionamento. Con l'aumentare della complessità e della diffusione dei sistemi di AI, monitorarne tutti i processi decisionali diventa sempre più difficile. Garantire la sicurezza dell'AI significa quindi accettare che possano verificarsi errori e incidenti e stabilire fin dove possano propagarsi. In

concreto, le aziende devono monitorare eventuali segnali di allarme, come un agente che utilizza uno strumento non autorizzato o un altro che perde parte delle istruzioni ricevute. Altri campanelli d'allarme possono essere un improvviso aumento dei costi o dei tempi di risposta, oppure l'interruzione del funzionamento di un sistema. Quando si verificano situazioni di questo tipo, è necessario verificare l'agente coinvolto o disattivarlo.
Perché è importante: nel 2027, le aziende dovranno concentrarsi sul contenimento dei rischi legati all'AI, anziché sulla sola spiegabilità dei suoi processi decisionali. Sarà inoltre necessario predisporre piani di controllo a livello aziendale che comprendano tutti gli agenti e i sistemi agentici, garantendo visibilità sulle interazioni tra agenti e sui primi segnali di eventuali anomalie tecniche.

3) Cybersecurity alla velocità delle macchine: gli attacchi informatici si muovono ormai alla stessa velocità
Oggi un agente AI può individuare autonomamente vulnerabilità nei software e trasformarle in attacchi reali, senza alcun intervento umano, anche quando non è stato progettato per svolgere questo tipo di attività. Sul fronte offensivo, il rischio è in aumento: l'AI potenzia le capacità di individuare vulnerabilità e sviluppare exploit, compresi quelli in grado di assumere il controllo di sistemi critici. Sul fronte della difesa, la superficie di attacco continua ad ampliarsi: ogni assistente AI, agente e sistema agentico introdotto crea un nuovo potenziale punto di accesso, mentre le capacità di rilevamento delle intrusioni non stanno migliorando con la stessa rapidità. Man mano che gli attacchi diventano sempre più automatizzati e industrializzati, una difesa informatica che attende la reazione di un analista umano è già in ritardo.
Perché è importante: nel 2027, con attacchi informatici che si muovono sempre più alla velocità delle macchine, anche le attività di sicurezza dovranno operare con la stessa rapidità. I Security Operations Center (SOC) dovranno affidare alle macchine le attività di classificazione e risposta agli incidenti, mentre le persone definiranno le regole, implementeranno i sistemi agentici e ne supervisioneranno il funzionamento. Questo cambiamento comporterà anche l'evoluzione verso una nuova generazione di Security Operations Center, in grado di rilevare una nuova minaccia nel giro di pochi minuti e intervenire per mitigarla molto più rapidamente.

4) Ricerca e sviluppo potenziati dall'AI agentica: l'R&D agentica supera i limiti delle capacità tradizionali
Nelle attività di ricerca e sviluppo, la capacità di ricercare, selezionare e convalidare diverse opzioni è stata tradizionalmente limitata dalle risorse disponibili e dalla capacità di effettuare test. L'AI cambia questo scenario in due fasi fondamentali: l'esplorazione, ovvero l'individuazione dell'idea giusta per un prodotto, e l'esecuzione, cioè la trasformazione di quell'idea in un prodotto concreto. Nella fase di esplorazione, finora le aziende sono state limitate dal numero di opzioni che potevano testare. L'AI supera questo limite, consentendo di esplorare un numero molto più ampio di possibilità, sia nell'ambito dei prodotti molecolari, come farmaci, sostanze chimiche e materiali, sia in quello dei prodotti fisici, come veicoli, macchinari e beni di consumo. Nella fase di esecuzione, l'AI interviene in ogni passaggio: gli agenti scrivono, testano e correggono il codice, mentre l'intelligenza artificiale supporta sempre più le attività di progettazione, simulazione, test e gestione del ciclo di vita dei prodotti.
Perché è importante: nel 2027, l'AI consentirà alle aziende di esplorare e valutare una gamma molto più ampia di possibilità, accelerando al contempo la fase di esecuzione. Nell'esplorazione, questo si tradurrà in maggiori capacità di individuare più rapidamente e valutare con maggiore precisione le opportunità più promettenti, come la scoperta di nuove molecole. Nella fase di esecuzione, gli ingegneri saranno sempre più supportati dall'AI, con una conseguente riduzione dei costi e un'accelerazione del time-to-market. Il modello operativo della ricerca e sviluppo dovrà adattarsi a un ecosistema basato su AI, agenti, dati e strumenti progettati nativamente per l'intelligenza artificiale.

5) Il commercio nell'era degli agenti AI: agenti protagonisti di entrambe le parti della transazione
Gli agenti AI stanno trasformando entrambi i versanti del commercio: gli acquisti e le vendite. Dal lato degli acquirenti, i consumatori possono chiedere a un assistente AI di individuare prodotti sulla base di criteri quali prezzo, disponibilità e tempi di consegna. In pochi secondi, l'agente può confrontare diversi rivenditori, raccogliendo informazioni sui prodotti, sui prezzi e sulle modalità di consegna. Dal lato dei venditori, i retailer stanno iniziando a utilizzare sistemi agentici per gestire le proprie attività, arricchire i cataloghi, adeguare prezzi e promozioni, rifornire le scorte e gestire il servizio clienti e i resi. Gli agenti stanno quindi diventando rapidamente parte integrante della transazione commerciale.
Perché è importante: nel 2027, le aziende dovranno sempre più rendere le proprie attività e offerte facilmente accessibili e comprensibili per gli agenti AI. Ciò significa mettere a disposizione dati chiari e strutturati su prodotti, prezzi, disponibilità delle scorte e consegne, oltre a sistemi che consentano di autenticare gli agenti autorizzati ad accedere e di impedire l'ingresso di quelli non autorizzati. Dal lato dei venditori, i sistemi agentici possono aumentare l'efficienza in

termini di costi e velocità delle attività commerciali. Allo stesso tempo, poiché l'AI influenza il modo in cui i consumatori scoprono, valutano e acquistano i prodotti, i brand dovranno assicurarsi che le proprie offerte rimangano visibili e pertinenti per gli assistenti AI, continuando al contempo a costruire la preferenza dei consumatori, la loro fidelizzazione e la fiducia nel marchio.

Capgemini

Capgemini è il partner per la trasformazione aziendale nell'era dell'AI. Aiutiamo le organizzazioni a immaginare e costruire un futuro intelligente e sostenibile, combinando AI, tecnologia e ingegno umano per trasformare il modo in cui operano, innovano e crescono. Grazie a competenze end-to-end che spaziano dalla strategia alla tecnologia, dall'ingegneria alle operations intelligenti, combiniamo una profonda conoscenza dei settori industriali con competenze all'avanguardia in ambito AI, cloud e dati, trasformando le ambizioni in risultati di business misurabili e scalabili. Supportata da un solido ecosistema di partner e forte di quasi 60 anni di esperienza, Capgemini è un'azienda globale responsabile e diversificata composta da oltre 410.000 persone in più di 50 paesi. Nel 2025 il Gruppo ha registrato ricavi complessivi pari a 22,5 miliardi di euro.

Make it real | www.capgemini.com