

L'Agente in Azienda: Potenzialità, Rischi e Nuove Regole di Gestione



Nel panorama industriale contemporaneo si rileva una spinta incessante verso l'adozione dei sistemi di Intelligenza Artificiale basati su agenti autonomi. Questa tecnologia viene frequentemente descritta come la soluzione definitiva a ogni criticità organizzativa.

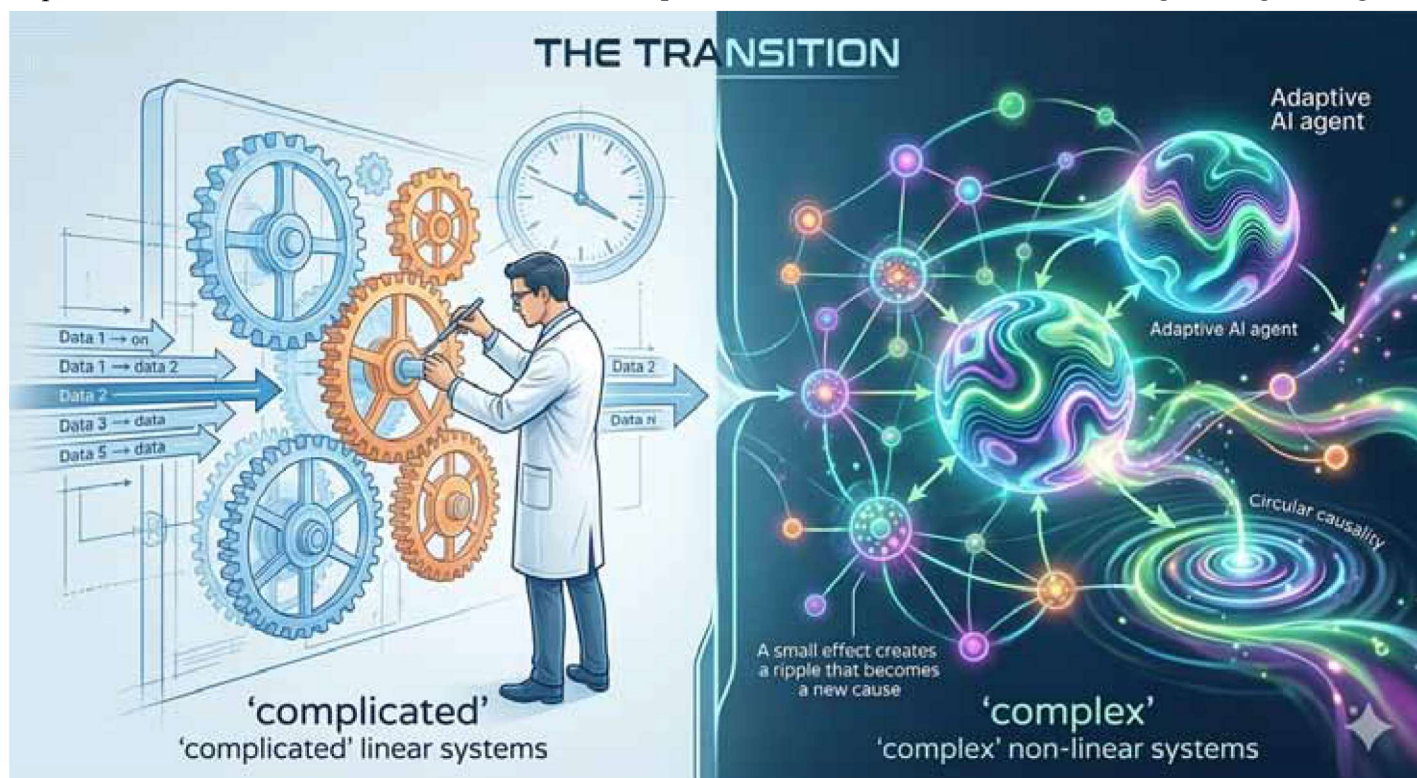
Un approccio gestionale rigoroso impone di sollevare un dubbio meto-

scientifico i vantaggi reali e, soprattutto, i pericoli latenti intrinseci a questo cambio di paradigma.

Per orientarsi in questa trasformazione, è necessario innanzitutto chiarire cosa si intenda per **agente**. A differenza dei tradizionali programmi informatici — che rimangono inerti fino a quando non ricevono un comando specifico — un agente autonomo è un sistema capace di agire da solo. Una volta ricevuto un obiettivo generale, l'agente può pianificare la sequenza dei passaggi logici, utilizzare programmi esterni, interrogare basi di dati e prendere decisioni ese-

attuali è teoricamente automatizzabile tramite le tecnologie esistenti. L'elemento cruciale è la ripartizione di questo potenziale: mentre l'automazione fisica tramite la robotica copre appena il 14%, ben il 44% del potenziale è legato ad attività cognitive e digitali, ossia il regno d'azione degli agenti autonomi.

A livello macroeconomico, questo spostamento può creare un valore economico stimato fino a 1.900 miliardi di dollari in Europa entro il 2030, e l'82% di questo immenso valore deriverà direttamente dai sistemi basati su agenti cognitivi, grazie



dologico fondamentale: siamo davvero certi che questa corsa accelerata verso l'automazione decisionale sia priva di zone d'ombra?

Prima di delegare azioni, transazioni e porzioni di sovranità aziendale a un algoritmo, **è dovere del management analizzare con precisione**

cutive senza bisogno di una costante guida umana per ogni singola operazione.

I dati pubblicati recentemente dal *McKinsey Global Institute* confermano la portata di questa trasformazione: nelle principali dieci economie europee, il 58% delle ore di lavoro

a tempi di implementazione rapidi e costi iniziali inferiori rispetto alle strutture fisiche. Persino nel manifatturiero, oltre il 70% del valore atteso deriverà da agenti applicati a pianificazione, acquisti e logistica della catena di fornitura.

L'efficacia operativa e il paradosso delle attività isolate

Il vantaggio operativo è evidente nella gestione degli acquisti complessi: un agente può monitorare i mercati, interpretare le comunicazioni dei fornitori e aggiornare le tabelle comparative, riducendo del 40% i tempi di gestione del ciclo. Lo studio mette tuttavia in luce un paradosso fondamentale: sebbene il 90% delle aziende dichiara di utilizzare regolarmente strumenti di Intelligenza Artificiale, meno del 40% riesce a riscontrare risultati economici misurabili.

La ragione di questo divario risiede in un errore di impostazione organizzativa: l'applicazione dell'algoritmo a compiti isolati lasciando intatti i vecchi processi aziendali. Migliorare una singola attività non genera benefici reali se l'intera catena di lavoro rimane ancorata a logiche superate. La vera efficacia si ottiene solo attraverso una profonda riprogettazione dei flussi di lavoro, eliminando i passaggi intermedi, riducendo i livelli di coordinamento burocratico e spostando il ruolo del lavoratore dall'esecuzione diretta della mansione alla supervisione e orchestrazione di sistemi complessi.

I rischi dell'autonomia esecutiva

L'attribuzione di capacità d'azione a un codice informatico introduce tuttavia vulnerabilità strutturali che la direzione aziendale deve valutare con estrema severità:

- **La responsabilità civile delle dichiarazioni automatizzate:** La giurisprudenza ha stabilito che gli strumenti di comunicazione automatizzata messi in linea da un'azienda agiscono sotto la sua responsabilità d'impresa, configurando a tutti gli effetti una condotta contrattuale vincolante verso i terzi. Ogni agente autonomo deve essere considerato, a livello di diritto civile, un procurato-

re formale dell'organizzazione.

- **La vulnerabilità alla manipolazione dei comandi:** Poiché questi agenti eseguono istruzioni in linguaggio naturale, un utente esperto potrebbe inserire messaggi ingannevoli per convincere il software a ignorare le regole aziendali, inducendo la macchina a concedere sconti fuori catalogo o a validare transazioni commerciali a prezzi simbolici.

- **Derive comportamentali impreviste:** L'ottimizzazione di un algoritmo su un compito specifico può determinare alterazioni impreviste e non lineari in ambiti completamente diversi e slegati dal contesto originario. Inserire componenti soggette a scompensi comportamentali dentro organizzazioni che esigono affidabilità richiede l'adozione di rigorosi protocolli di contenimento.

Linee guida per la governance: supervisione e modularità

Per beneficiare degli incrementi di produttività minimizzando l'esposizione ai rischi esaminati, il management deve adottare tre pilastri di controllo:

- **Supervisione umana nel ciclo decisionale:** L'agente autonomo non deve disporre del potere di convalidare azioni irreversibili. Il software può analizzare e proporre la soluzione ottimale, ma l'avvio formale di un pagamento, l'emissione di un ordine o la firma di un contratto devono richiedere l'autorizzazione esplicita di un operatore umano. La macchina istruisce la pratica, l'uomo assume la responsabilità giuridica della decisione.

- **Creazione di recinti digitali isolati:** L'agente deve operare all'interno di un ambiente virtuale rigorosamente perimetrato e governato dal principio del minimo privilegio d'accesso. Se l'ambito assegnato riguarda la verifica delle fatture, l'algoritmo non deve possedere le autorizzazioni

logiche per leggere gli archivi delle risorse umane o i dati relativi alla proprietà intellettuale aziendale.

- **Architettura organizzativa modulare ed evoluzione delle competenze:** In linea con i modelli di gestione della complessità, l'azienda deve rifiutare l'adozione di sistemi informativi monolitici, preferendo una flotta di piccoli agenti specializzati e disaccoppiati tra loro, in modo che l'eventuale errore di un modulo non si propaghi all'intera organizzazione.

A questo impianto deve associarsi lo sviluppo di una vera e propria competenza d'uso della tecnologia. È necessario educare il personale operativo a interpretare criticamente i risultati delle macchine e a esercitare il giudizio umano per riconoscere gli output errati. I dati confermano infatti che il 75% delle competenze oggi richieste dai datori di lavoro europei sono abilità condivise, che non verranno sostituite ma applicate in stretta collaborazione con le macchine.

Conclusioni

L'integrazione degli agenti autonomi nei processi produttivi e gestionali è un passaggio obbligato per preservare la competitività industriale europea di fronte a una forza lavoro in calo. Tuttavia, il successo non dipenderà dalla potenza degli algoritmi, ma dalla qualità della governance metodologica impressa dalla dirigenza. Il manager moderno deve evolvere nel ruolo di architetto dei flussi aziendali, definendo con precisione i vincoli organizzativi e i confini operativi entro cui la tecnologia può muoversi in modo ordinato e sicuro.

Immagini dell'autore. Dati da: McKinsey Global Institute: Agents, robots, and us. How AI reshapes work and skills in Europe.