La governance della Ai in azienda passa dalle competenze umane

Innovazione. La Shadow Ai minaccia la sovranità del dato e mette a rischio di errori e debiti tecnici e legali occulti. Ma le proibizioni non servono

Massimo Chiriatti

La storia dell'informatica aziendale è una storia di tensioni dialettiche tra il centro e la periferia, in particolare, tra centralizzazione e decentralizzazione. Tra chi controlla l'infrastruttura e chi la deve usare per produrre valore. Negli anni passati abbiamo imparato a convivere con lo Shadow It, ovvero l'utilizzo di software e dispositivi mobili all'ombra dai responsabili tecnologici, e comunque non approvati. Oggi ci troviamo di fronte a una mutazione ben più insidiosa e complessa: lo Shadow AI.

Definiamo le cause più probabili.

Siamo di fronte a un fenomeno in cui l'Ai generativa, accessibile a chiunque disponga di un browser, viene impiegata per svolgere compiti critici all'insaputa dell'organizzazione. La deduzione logica è immediata: se l'accesso alla potenza computazionale è diventato privo di attrito, allora il controllo centralizzato tradizionale non è più un argine sufficiente.

Chi usa in questo modo l'Ai non lo fa con intenti dolosi, piuttosto segue un principio di efficienza economica individuale, come a dire, sta cercando di massimizzare la propria produttività, colmando il divario tra la domanda di velocità imposta dal mercato e la risposta spesso lenta dei processi interni. Purtroppo, con tal modo di operare, ignora cosa mette a rischio con le sue operazioni.

Delineiamo le possibili conseguenze. Quando portiamo questi strumenti nell'ombra, ossia al di fuori del perimetro della governance aziendale, esponiamo l'organizzazione a tre rischi esistenziali che non possono essere ignorati.

Il primo è, naturalmente, la sovranità del dato. Inserire dati riservati in un prompt di un modello pubblico equivale, in molti casi, a cedere quei dati al fornitore del modello per l'addestramento futuro. È una perdita di proprietà intellettuale silenziosa e continua, in tal modo il core business dell'azienda è in pericolo.

Il secondo rischio è quando si dimentica che la macchina calcola non pensa. Produce contenuti senza rendersi conto di farlo. Nell'ombra, decisioni strategiche potrebbero essere prese basandosi su inferenze statistiche errate, generate da una macchina che non ha una piena comprensione del contesto di ciò che ha prodotto. Se deleghiamo il pensiero alla macchina senza supervisione, stiamo abdicando alla nostra responsabilità umana.

Il terzo rischio è il debito tecnico e legale occulto. Un codice generato da un'Ia senza licenza chiara, o un testo che viola copyright, entra nei sistemi aziendali senza tracciabilità. Quando, inevitabilmente, arriverà il momento di rendere conto di quegli asset, l'azienda si troverà a dover gestire passività di cui ignorava l'esistenza.

Ipotizziamo le soluzioni più preferibili. La proibizione, bloccare gli accessi, la storia del digitale ce lo insegna, non funziona. La risposta non è mai stata con l'introduzione di ulteriore tecnologia, infatti i risultati migliori si ottengono con innovazioni organizzative, e soprattutto culturali.

Dobbiamo spostare l'asse dall'inutile controllo a priori alla competenza. Lo Shadow AI prospera dove manca una cultura diffusa dell'IA. Se i dipendenti usano strumenti non approvati, è spesso perché l'azienda non ha fornito alternative valide e sicure. Le aziende dovrebbero fornire "sandbox" sicure, ambienti protetti dove i modelli sono istanziati privatamente, dove i dati non escono dal perimetro aziendale e dove l'output è sottoposto a verifica.

È necessario, inoltre, un ritorno ai fondamentali del pensiero critico. L'adozione dell'IA richiede più umanesimo, non meno. Dobbiamo formare le persone non tanto all'uso dello strumento (l'interfaccia è ormai il linguaggio naturale, accessibile a tutti), quanto alla valutazione del risultato. La competenza tecnica deve evolversi in competenza epistemologica: saper distinguere una correlazione

statistica da un nesso causale, saper riconoscere un bias, saper valutare l'etica di un output.

Pertanto, possiamo ridefinire lo Shadow AI come un segnale di mercato interno. Ci indica che la fame di automazione cognitiva è immensa. La vera sfida per i C-level è portare l'IA dall'ombra alla luce, dove può essere governata, misurata e, soprattutto, diretta dall'intenzione umana. Tornare agli anni 70 dove c'erano solo i sistemi centralizzati e tra le mani c'era solo un terminale, non un personal computer, di certo non avremmo rischi di sicurezza in periferia, ma neanche creatività e responsabilità che, a differenza del calcolo, non è delegabile. E la responsabilità è l'unica realtà oggettiva che ci distingue, e sempre ci distinguerà, dalle macchine.

Chief Technology & Innovation Officer, Italy, Lenovo