Microsoft 365 Copilot

Come garantire la sicurezza dei dati nell'era dell'IA

Una guida per i leader IT

E-Book

Questa guida è destinata ai leader IT che devono promuovere l'adozione dell'IA e proteggere al tempo stesso i dati dell'organizzazione. Aiuterà a comprendere meglio i rischi che l'IA pone in termini di sicurezza e privacy dei dati, offrendo contemporaneamente gli insights necessari per gestire con sicurezza la trasformazione dell'azienda verso l'IA.

Indice

01

Le nuove regole del lavoro basato sull'IA

L'IA generativa apre nuove porte all'innovazione e aiuta i team a lavorare in modo più veloce e intelligente che mai. Per le organizzazioni lungimiranti, l'IA non è solo una nuova tendenza tecnologica, ma un imperativo di business, essenziale per il modo di operare delle aziende, di offrire valore e di promuovere un vantaggio competitivo.

Tuttavia, questa rapida adozione comporta sfide nuove e amplificate che i leader IT devono affrontare e controllare in modo proattivo. I sistemi di IA possono cercare attivamente e combinare le informazioni nell'intero ecosistema di dati, portando i rischi per la sicurezza oltre i limiti degli strumenti tradizionali. Nonostante la rapida espansione dell'IA, solo l'**1%** delle organizzazioni dichiara di averla completamente integrata nei flussi di lavoro con i protocolli di sicurezza appropriati.[1] Grazie all'implementazione di solide misure di sicurezza e governance fin dalle prime fasi del percorso verso l'IA, il team può proteggere efficacemente i dati sensibili, mantenere i requisiti di compliance e tutelare le informazioni dell'organizzazione, promuovendo al tempo stesso l'innovazione.

L'ondata di adozioni dell'IA è arrivata

02

Informazioni sull'impatto dell'IA sulla sicurezza dei dati

Prima di affrontare le specifiche problematiche, è importante capire in che modo l'IA ha cambiato radicalmente il panorama della sicurezza dei dati. A differenza del software tradizionale che accede ai dati solo in risposta a una specifica istruzione, l'IA generativa elabora, analizza e crea attivamente i contenuti in base a tutte le informazioni che riceve.

Questa differenza è significativa per diversi motivi:

- Gli strumenti di IA possono individuare connessioni tra i dati di cui gli esseri umani potrebbero non accorgersi
- Possono sintetizzare automaticamente le informazioni provenienti da più origini
- Possono generare nuovi contenuti che includono elementi provenienti da input sensibili

Gli strumenti di sicurezza tradizionali probabilmente non sono stati progettati tenendo conto di queste funzionalità. Mentre il software convenzionale segue percorsi prevedibili quando accede ai dati, l'IA può percorrere strade inedite nell'ecosistema delle informazioni, rischiando di esporre i dati sensibili in modi imprevisti.

Questo cambiamento radicale richiede nuovi approcci alla sicurezza e alla governance dei dati, in grado di affrontare le specifiche modalità a cui l'IA fa ricorso per interagire con le risorse informative dell'organizzazione.

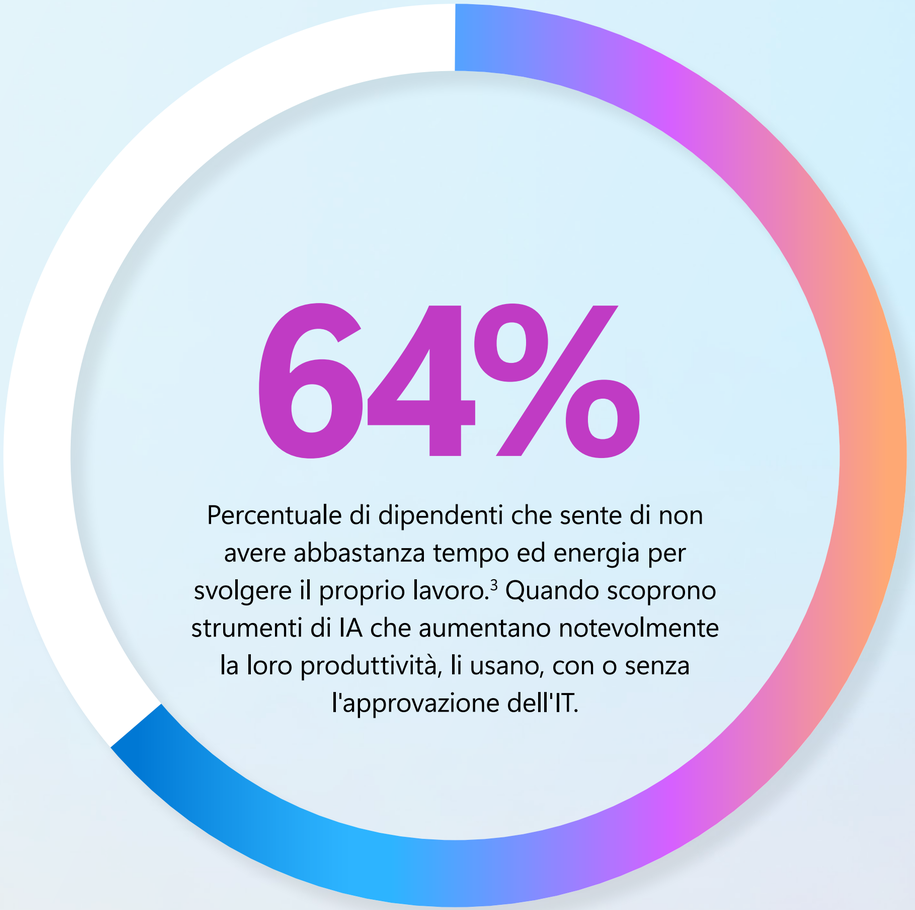
03

La sfida della shadow AI

Indipendentemente dalla fase del percorso di adozione dell'IA in cui ti trovi, è molto probabile che i tuoi dipendenti stiano già usando delle soluzioni personali, creando la cosiddetta "shadow AI".

Questo uso non autorizzato causa importanti punti ciechi nella postura di sicurezza dell'azienda. Quando i dipendenti condividono i dati aziendali con sistemi di IA esterni, aggirano i controlli di sicurezza esistenti e creano vulnerabilità che la maggior parte delle organizzazioni non è pronta ad affrontare.

La shadow AI non è solo un problema di sicurezza, ma potrebbe essere un sintomo di esigenze di produttività non soddisfatte nella tua organizzazione. Quando i dipendenti adottano strumenti non autorizzati, evidenziano aspetti dei sistemi ufficiali che non soddisfano i loro requisiti. Per gestire la shadow AI serve una governance più forte e soluzioni di produttività avanzate.



Perché emerge la shadow AI:

- I dipendenti non vedono l'ora di aumentare la produttività grazie alle straordinarie capacità dell'IA
- I workload quotidiani superano sempre di più il tempo e l'energia disponibili
- Sui team vengono esercitate enormi pressioni affinché raggiungano maggiori risultati con le stesse risorse
- Gli strumenti di IA di tipo consumer offrono soluzioni immediate senza alcun ostacolo di approvazione
- I processi ufficiali di approvvigionamento IT non possono eguagliare il ritmo dell'innovazione

I rischi della shadow AI:

- Nessuna visibilità sui dati aziendali elaborati dai sistemi di IA esterni
- Nessuna garanzia che le informazioni riservate non vengano conservate
- Nessuno standard di sicurezza coerente per le diverse piattaforme di IA
- Nessuna possibilità di controllo ai fini della compliance
- Nessuna integrazione con l'infrastruttura di sicurezza esistente

Considera questo scenario:

Un analista finanziario non riesce a venire a capo di un foglio di calcolo complesso e decide di caricarlo in uno strumento di IA non autorizzato per ottenere aiuto. Il foglio di calcolo contiene dati finanziari dei clienti, metriche interne e proiezioni. L'analista ottiene l'aiuto di cui ha bisogno, ma i dati finanziari sensibili dell'organizzazione ormai sono fuoriusciti dal perimetro di sicurezza, completamente invisibili ai sistemi di monitoraggio.

04

La realtà BYOAI

Senza indicazioni chiare da parte della leadership, i dipendenti stanno adottando sempre più l'IA autonomamente, con il **78%** degli utenti di IA che usa un approccio "Bring Your Own AI" (BYOAI), ossia porta i propri strumenti di IA al lavoro.[2] Questa tendenza è ancora più pronunciata nelle piccole e medie imprese, dove l'**80%** dei dipendenti adotta procedure BYOAI.[2]

Questo approccio non autorizzato presenta diversi lati negativi. I dipendenti spesso usano l'IA di nascosto: il **52%** è riluttante ad ammetterne l'uso per attività importanti e il **53%** teme che il ricorso all'IA lo faccia sembrare più sostituibile.[2] Questo riserbo non solo impedisce alle organizzazioni di cogliere tutti i vantaggi di un'implementazione strategica dell'IA, ma crea anche gravi vulnerabilità di sicurezza in un ambiente in cui, a detta dei leader, la cybersecurity e la privacy dei dati hanno la **priorità assoluta**.[2]

A causa della diffusione e dell'inevitabile crescita dell'IA, la questione centrale non è se consentire l'IA nell'organizzazione, ma come fornire una soluzione sicura in grado di soddisfare le esigenze dei dipendenti, garantendo al tempo stesso la protezione dei dati aziendali.

05

Il ginepraio dei regolamenti

I framework e le leggi su privacy e sicurezza dei dati creano un altro livello di complessità quando si adotta l'IA. Alcuni framework sono specificamente progettati per la governance dell'IA, mentre altri hanno applicazioni più ampie che incidono ancora sulla gestione delle informazioni e le sanzioni per le violazioni rimangono gravi.

Quando i dipendenti usano gli strumenti di IA senza un'adeguata supervisione, potrebbero involontariamente creare violazioni alla compliance. L'IA aumenta questo rischio perché può accedere alle informazioni soggette a regolamenti, combinarle ed esporle in modi non previsti dalle tecnologie tradizionali.

Regolamenti principali inerenti l'uso dell'IA:

GDPR

Il Regolamento generale sulla protezione dei dati dell'Unione europea conferisce alle persone il controllo sui propri dati personali e richiede un consenso esplicito per il loro trattamento

Regolamento UE sull'IA

Il framework completo dell'Unione europea specificamente progettato per regolare i sistemi di IA in base ai loro livelli di rischio

HIPAA

Questa legge federale degli Stati Uniti per il settore sanitario stabilisce rigidi standard per la gestione delle informazioni sanitarie protette

AI Risk Management Framework di NIST

Queste linee guida degli Stati Uniti applicabili su base volontaria aiutano le organizzazioni ad affrontare i rischi nella progettazione, nello sviluppo e nella distribuzione dei sistemi di IA

I rischi di compliance associati all'IA:

- Elaborazione dei dati dei clienti su server al di fuori delle aree approvate
- Informazioni personali usate senza il consenso appropriato
- Dati sensibili mantenuti nei sistemi senza i controlli di conservazione appropriati
- Nessun audit trail sulle modalità di accesso e utilizzo delle informazioni protette
- Contenuti generati dall'IA che violano i requisiti di compliance specifici del settore

Queste violazioni possono portare a gravi conseguenze:

- Gravi sanzioni finanziarie (le sanzioni del GDPR possono raggiungere il **4%** del fatturato globale)[4]
- Requisiti che prevedono la comunicazione delle violazioni dei dati alle parti interessate
- Azione legale delle parti coinvolte
- Danno alla reputazione dell'azienda e alla fiducia dei clienti

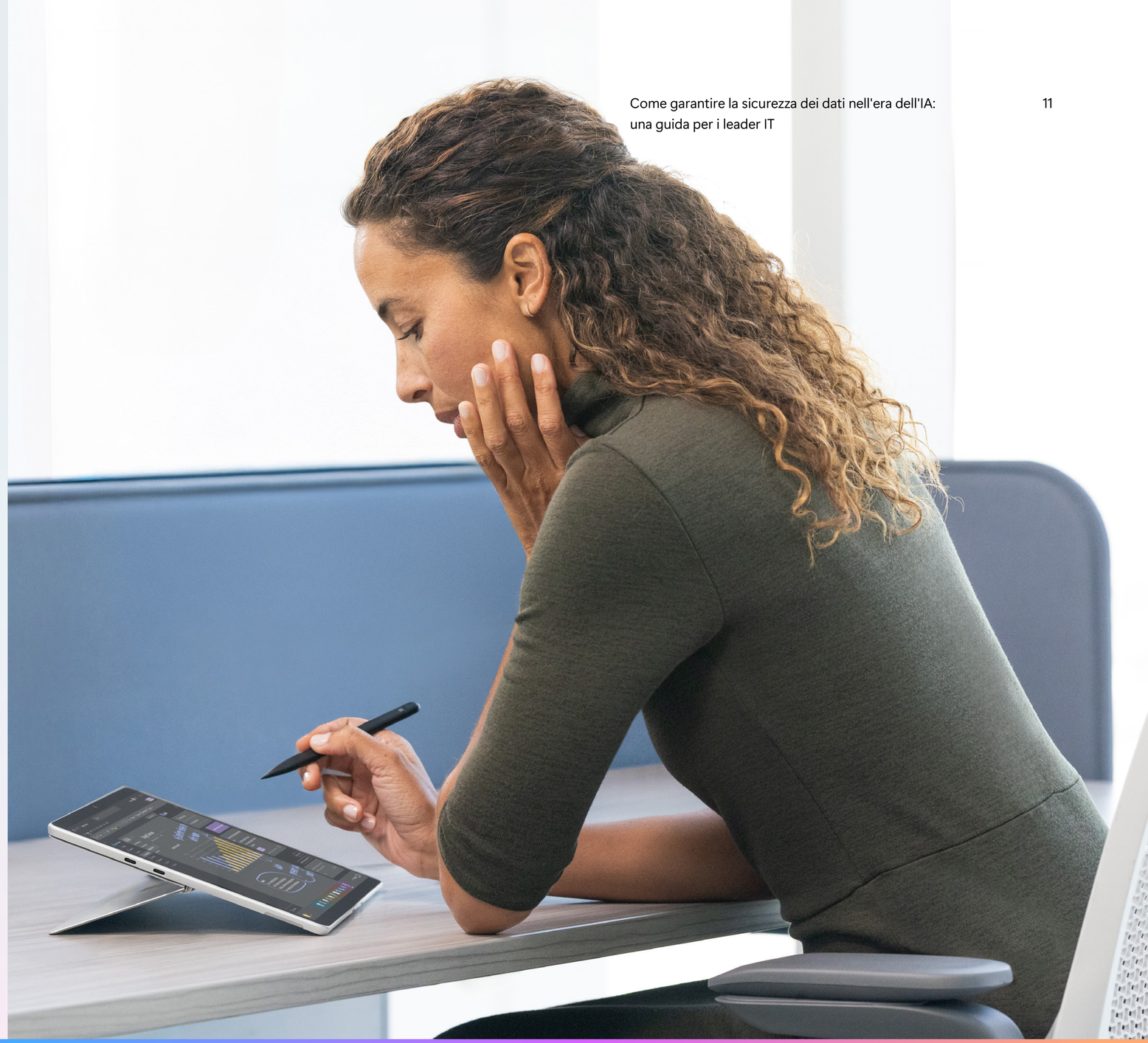
Con la diffusione dell'IA in tutta la tua organizzazione, hai bisogno di una governance che aiuti le persone a lavorare in modo efficiente, garantendo al tempo stesso la compliance dell'organizzazione ai regolamenti inerenti al tuo business e ai tuoi clienti.

06

Un framework incentrato sulla sicurezza per la valutazione delle soluzioni di IA

Di fronte ai rischi importanti posti dalla shadow AI, dalla tendenza BYOAI e dai regolamenti, hai bisogno di un approccio strutturato alla valutazione delle soluzioni di IA, che garantisca alla tua organizzazione la capacità di promuovere l'innovazione, proteggendo al tempo stesso i dati sensibili e assicurando la compliance ai requisiti normativi in continuo cambiamento.

Il framework seguente suggerisce sei semplici domande per valutare se una piattaforma di IA soddisfa tutte queste esigenze.



Domanda 1

La piattaforma offre un livello di sicurezza aziendale fin dalle basi?

Con la soluzione giusta, la sicurezza passa dalla semplice reazione ai problemi, una volta che si sono verificati, alla ricerca proattiva delle vulnerabilità nei dati dell'organizzazione, prima che diventino problemi più gravi.

Cerca soluzioni che:

- Forniscono visibilità in tempo reale sull'intero ecosistema di dati
- Identificano automaticamente i rischi potenziali per i dati prima che si trasformino in incidenti
- Proteggono le informazioni sensibili a ogni livello

Domanda 2

La piattaforma può adottare e migliorare facilmente i controlli di sicurezza esistenti?

I criteri di sicurezza della tua organizzazione devono integrarsi perfettamente con l'IA. Il provider di soluzioni di IA deve rispettare e integrarsi nei framework di sicurezza esistenti, senza richiedere di crearne di nuovi.

Cerca soluzioni che:

- Adottano senza problemi i criteri di sicurezza, le etichette di riservatezza e le impostazioni di protezione delle informazioni esistenti
- Applicano controlli di accesso granulari a livello dei singoli soggetti, in modo che nessun utente possa accedere a dati per i quali non ha l'autorizzazione
- Segnalano attivamente i tentativi di alterare i controlli di accesso

Domanda 3

La piattaforma include controlli integrati per la privacy e la governance?

Poiché gli strumenti di IA funzionano in modo più proattivo, anche le misure di sicurezza devono essere proattive. L'implementazione di una governance avanzata dei dati crea confini chiari in cui i dipendenti possono innovare in tutta sicurezza senza mettere a rischio le informazioni sensibili.

Cerca soluzioni che:

- Centralizzano la governance dell'IA applicando criteri automatizzati a tutte le attività
- Includono il rilevamento precoce della potenziale condivisione eccessiva dei dati
- Si allineano ai framework normativi per garantire un uso conforme dell'IA

Domanda 4

La piattaforma può essere distribuita in modo coerente in tutta l'organizzazione?

Ogni dipendente della tua organizzazione ha il suo stile di lavoro e le sue pianificazioni e potrebbe lavorare ovunque nel mondo. L'IA deve offrire vantaggi a tutti.

Cerca soluzioni che:

- Offrono una configurazione ottimale e un'adozione semplice dell'IA nei flussi di lavoro quotidiani
- Forniscono un accesso flessibile, dalla chat di IA gratuita alle soluzioni scalabili per gli agenti
- Aiutano i dipendenti ad acquisire dimestichezza con l'IA e a integrarla nel loro lavoro

Domanda 5

La piattaforma si integra in modo ottimale nei framework esistenti?

La tua azienda attualmente opera con una propria infrastruttura digitale di programmi software, app e altro ancora.

Cerca soluzioni che:

- Si integrano senza problemi con gli strumenti e i programmi in uso per ridurre al minimo le interruzioni
- Offrono un'esperienza di IA continua in tutte le app, che consente di passare senza ostacoli tra i diversi strumenti
- Automatizzano e ottimizzano le attività nei flussi di lavoro esistenti

Domanda 6

Gli utenti hanno tutto il necessario per innovare?

L'obiettivo principale dell'IA è la trasformazione del modo di lavorare. Non si tratta solo di automazione, ma di migliorare la produttività e promuovere l'innovazione.

Cerca soluzioni che:

- Trasformano le perdite di tempo in processi ottimizzati
- Automatizzano le attività ripetitive
- Consentono ai lavoratori di risparmiare tempo e concentrarsi sulle priorità

07

Microsoft 365 Copilot: una IA affidabile

Microsoft 365 Copilot è la soluzione di IA generativa creata per garantire sicurezza, governance e controlli di accesso affidabili, assicurando una distribuzione sicura e un'innovazione duratura. Aumenta la produttività con strumenti intuitivi come Copilot Chat, che ti affianca nel lavoro, e Copilot Studio, che permette al tuo team di creare agenti di IA personalizzati senza alcuna competenza di codifica.

Copilot si integra perfettamente nell'ambiente Microsoft 365, ereditando autorizzazioni utente, etichette di riservatezza, criteri di prevenzione della perdita dei dati e requisiti di residenza dei dati geografici, senza necessità di ulteriori configurazioni. Incorporando l'IA negli strumenti già usati dai dipendenti, Copilot mitiga i rischi per la sicurezza mantenendo i dati all'interno del tuo ambiente affidabile Microsoft 365.

Grazie agli impegni di Microsoft, la tua organizzazione mantiene il controllo:

- I dati inattivi e in transito sono protetti
- I tuoi dati non vengono usati per il training dei modelli di IA
- Decidi tu quali informazioni inserire nel cloud
- Puoi contare sulla protezione contro i rischi associati alla sicurezza dell'IA e al copyright

Strumenti di governance appositamente progettati, come Sistema di controllo Copilot e Gestione avanzata di SharePoint, offrono ai team IT la visibilità, i controlli e i log di controllo necessari per assicurare la compliance.

Con Microsoft 365 Copilot, non devi scegliere tra innovazione e sicurezza: puoi averle entrambe.

08

Il percorso sicuro verso la trasformazione con l'IA

La rivoluzione dell'IA presenta ai leader IT un'opportunità unica per offrire valore strategico bilanciando innovazione e sicurezza.

Implementando strumenti di IA sicuri come Microsoft 365 Copilot, puoi fornire ai tuoi dipendenti strumenti per una maggiore produttività, eliminando al tempo stesso i rischi della shadow AI. Il percorso da seguire è promuovere l'innovazione in modo sicuro. La tua leadership nell'adozione sicura dell'IA posizionerà l'IT come promotore della trasformazione, aiutando la tua organizzazione a prosperare in questa nuova era mantenendo i dati sicuri e conformi.

Inizia con Microsoft 365 Copilot

Fonti:

[1] "Superagency in the workplace: Empowering people to unlock AI's full potential", McKinsey & Company, 28 gennaio 2025. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] "L'IA è arrivata al lavoro. Ora inizia la parte difficile", Microsoft Work Trend Index, 8 maggio 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] "L'IA risolverà il problema del lavoro?", Microsoft Work Trend Index, 9 maggio 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", Parlamento Europeo e Consiglio dell'Unione Europea, 27 aprile 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.