Technology

Shadow AI

una minaccia per la cybersecurity delle imprese

ANDERSEN®

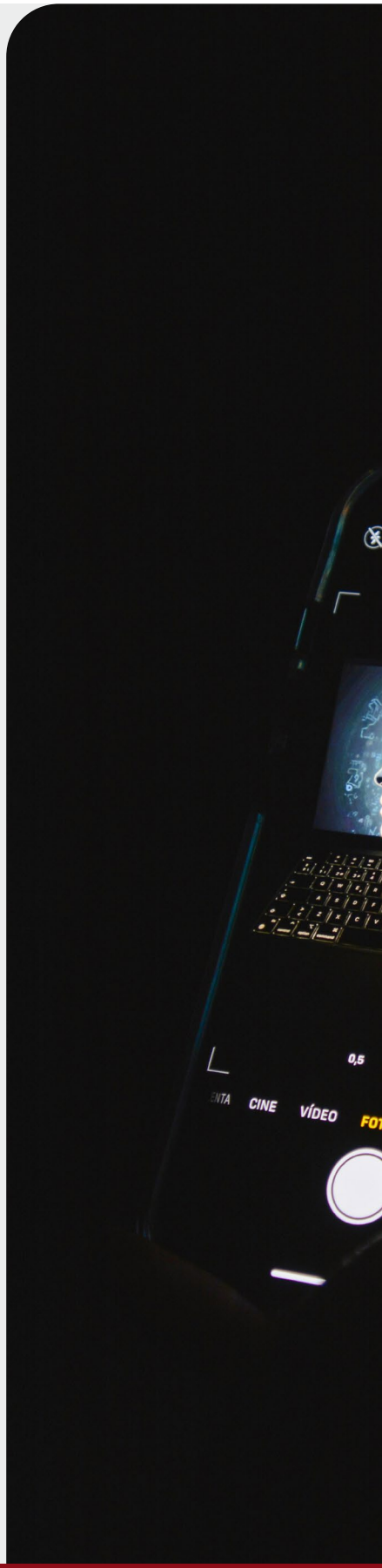
La diffusione della GenAI

Negli ultimi due anni si è assistito ad una grande diffusione della **GenAI** o **AI Generativa**.

Con tale termine si identifica un tipo di **Intelligenza Artificiale** che utilizza algoritmi di deep learning per generare nuovi contenuti come immagini, video e musiche in risposta al prompt o alla richiesta di un utente. Si tratta di una AI basata tipicamente su foundation model per l'interpretazione del linguaggio naturale, ovvero Large Language Models, della cui famiglia fanno parte gli stessi GPT4 di Open AI, Gemini di Google, Copilot di Microsoft, Llama di Meta e la cinese DeepSeek AI della cinese Deep Seek.

Nel contesto aziendale l'AI Generativa ha avuto e ha attualmente un forte sviluppo, complice l'utilizzo di tale tecnologia per la gestione della knowledge base aziendale. Diverse imprese, infatti, la utilizzano per automatizzare la creazione, l'organizzazione e l'aggiornamento delle informazioni aziendali.

Secondo una ricerca della società di consulenza aziendale McKinsey, un terzo delle organizzazioni utilizza già regolarmente l'AI generativa in almeno una funzione aziendale[1]. L'analista di settore Gartner, inoltre, prevede che entro il 2026 oltre l'80% delle organizzazioni del settore pubblico e privato avrà implementato applicazioni di AI generativa o utilizzato interfacce di programmazione delle applicazioni (API) di AI generativa[2].

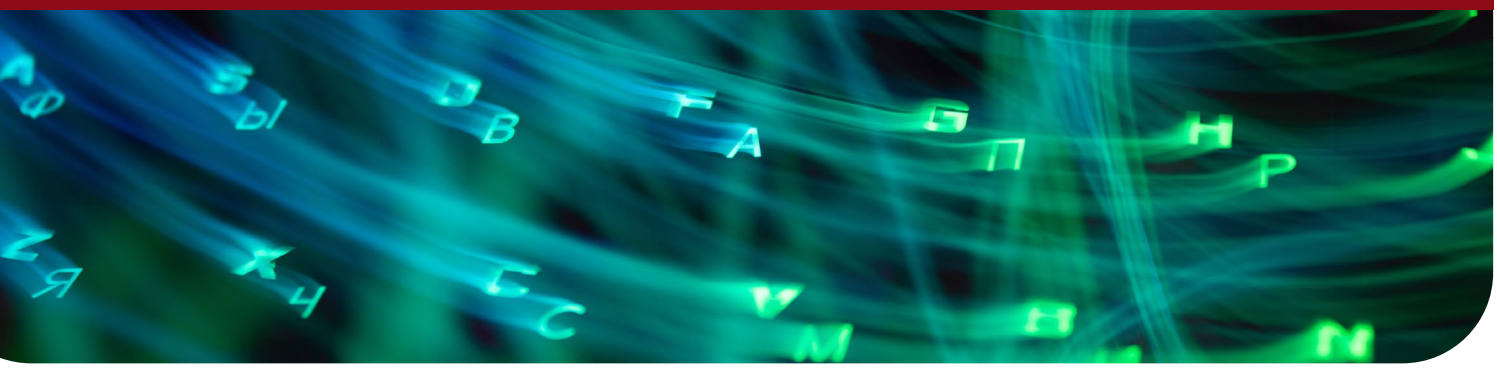


Autori dell'approfondimento
Paola Finetto
Partner
paola.finetto@it.andersen.com

Nicolò Bottura
Avvocato
nicolo.bottura@it.andersen.com

[1] Vd. The state of AI in 2023: Generative AI's breakout year, McKinsey, 1° agosto 2023

[2] Vd. Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026, Gartner, 11 ottobre 2023



I rischi derivanti dall'utilizzo della GenAI: la Shadow AI

Ci sono tuttavia dei **rischi** invisibili che derivano dall'utilizzo incontrollato della GenAI al di fuori delle strategie e delle procedure aziendali, i quali possono esporre le organizzazioni a **minacce** per le proprie infrastrutture tecnologiche e per i dati trattati, oltre al rischio di non conformità alle normative (tra cui GDPR e NIS 2) e di inefficienza operativa.

Tra le minacce divenute comuni a causa della proliferazione di piattaforme basate sull'intelligenza artificiale vi è l'esposizione ad attacchi informatici sofisticati e difficili da individuare con strumenti tradizionali, potenziati da un aumento delle tecniche di social engineering con cui gli hacker creano mail di phishing[3] e deepfake realistiche, inducendo i dipendenti a condividere credenziali di accesso e informazioni riservate.

Dietro un attacco informatico "in gran stile" può celarsi anche la **Shadow AI** o AI Ombra che si verifica, ad esempio, in tutti quei i casi in cui un dipendente utilizza la GenAI per scrivere o tradurre velocemente un documento senza rispettare le policy aziendali oppure si serve dell'intelligenza artificiale per analizzare i dati di coinvolgimento sui social media, o ancora per individuare nei CV determinati dati utili per elaborazione statistica.

Shadow AI
Uso non autorizzato di qualsiasi strumento o applicazione di intelligenza artificiale (IA) da parte di dipendenti o utenti finali senza l'approvazione formale o la supervisione del dipartimento ICT o comunque del management.

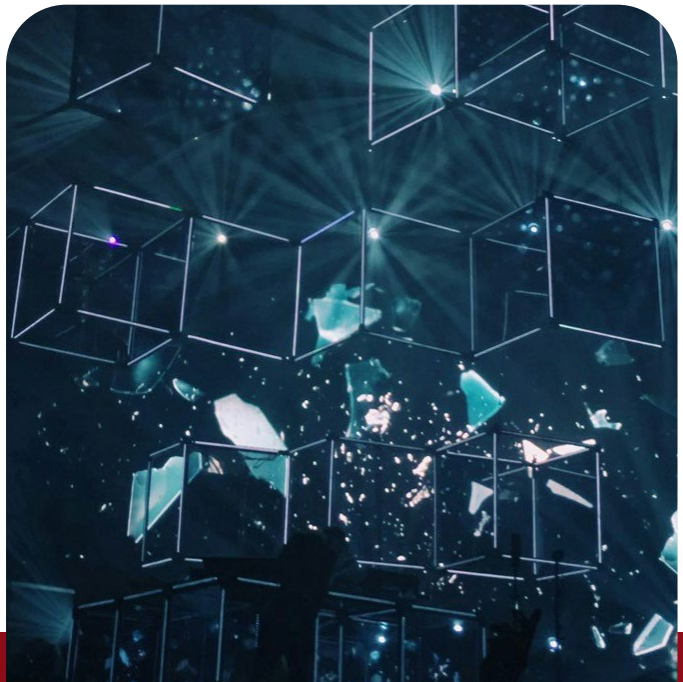
Ciò considerato, viene naturale chiedersi: **perché il fenomeno dello Shadow AI si sta diffondendo? Quali sono i rischi che ne derivano? Come possono fare le imprese per mitigarli?**

La diffusione di strumenti AI user-friendly, la percezione che i sistemi informatici aziendali siano obsoleti e che i processi aziendali costituiscano un ostacolo all'innovazione, unita alla necessità di adottare soluzioni immediate senza particolari competenze tecniche per sviluppare progetti sempre più ambiziosi e migliorare la produttività aziendale sta contribuendo ad accrescere il fenomeno Shadow AI.

Al settembre 2024, oltre un terzo (38%) dei dipendenti ha ammesso di condividere informazioni aziendali riservate con strumenti di intelligenza artificiale senza il permesso dei propri datori di lavoro[4].

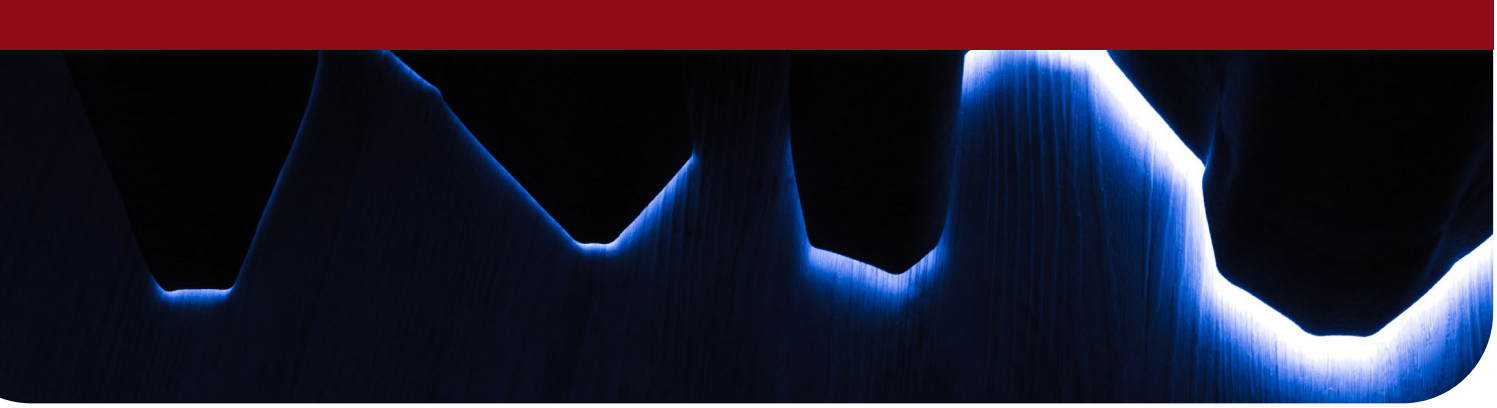
Di fronte a tale dato diviene necessario prendere coscienza della necessità di un **approccio risk based** (ormai alla base delle più importanti normative europee, tra cui il GDPR e l'AI ACT) rispetto alla gestione delle nuove tecnologie all'interno delle organizzazioni per ridurre i rischi.

A tal proposito, è importante andare a monte, ovvero definire i rischi che possono derivare dalla Shadow AI per capire come mitigarli al meglio.



[3] Secondo quanto riportato nel report pubblicato da Acronis per il secondo semestre del 2024, Acronis Executive Summary Cybert Threats Report 2024, il 74% degli attacchi informatici avviene attraverso il phishing mentre il 22% tramite social engineering, in crescita del 7% rispetto all'anno 2023 anche a causa dell'utilizzo della GenAI da parte dei criminali informatici

[4] Over a Third of Employees Secretly Sharing Work Info with AI, Infosecurity Magazine, 26 September 2024;



I rischi della Shadow AI

I principali rischi derivanti dalla Shadow AI riguardano infatti i seguenti ambiti:

Cybersecurity & Data Protection: il verificarsi di **incidenti di sicurezza o di violazioni di dati personali (data breach[5])** dovuti, nella maggior parte dei casi, all'introduzione di un software AI non autorizzato con cui vengono condivise informazioni personali o aziendali riservate

Legal & Compliance: la **violazione delle procedure aziendali e la non conformità normativa**

Operational: l'**inefficienza operativa** dovuta alla diversità delle soluzioni informatiche e alla difficoltà relativa al monitoraggio delle vulnerabilità e delle minacce

Intellectual property: la **violazione del copyright**, che si può verificare quando un dipendente utilizza l'intelligenza artificiale per la generazione di contenuti, utilizzando inconsapevolmente materiale protetto da copyright

Reputational: il **danno alla reputazione aziendale**.

Tutti questi aspetti hanno impatti rilevanti sull'operatività, l'efficienza dei processi, la reputazione e di conseguenza, il business generale.

Il dato che ad oggi più preoccupa è che le organizzazioni impiegano ancora in media **73 giorni**[6] per gestire un incidente di sicurezza, con difficoltà tali da doversi affidare a terze parti per identificare e monitorare il rischio cyber, ritenuto - secondo il report pubblicato da Allianz nel 2025[7] - il rischio più impattante per il business a livello globale.

Alla luce di tali considerazioni, diviene importante per un'impresa capire come proteggersi da tale fenomeno e dai rischi da esso derivanti per mantenere così la propria **business continuity**.

Strategie di governance e approccio risk based per aumentare la resilienza

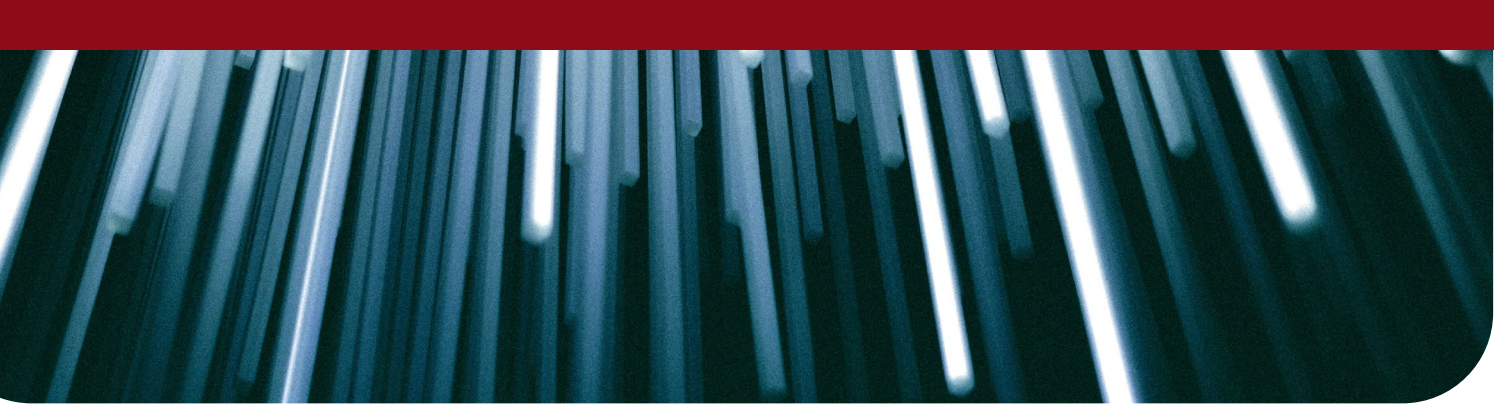
Per garantire che l'impresa resti resiliente, rafforzando al contempo la fiducia degli utenti, non basta acquisire consapevolezza del pericolo.

È necessario, infatti, adottare delle procedure aziendali chiare per regolare l'uso dell'intelligenza artificiale, essere conformi alle normative, valutare i rischi derivanti dall'utilizzo di determinati strumenti di intelligenza artificiale e alfabetizzare le persone che fanno parte dell'azienda attraverso la formazione. Fondamentale in tal senso diviene la creazione di un **sistema di compliance integrato**, grazie all'apporto multidisciplinare delle funzioni aziendali interne.

[5] *Per data breach, ai sensi dell'art. 33 GDPR, si intende una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*

[6] *Cost of a Data Breach Report 2024, IBM, 2024*

[7] *Vd. Allianz Risk Barometer 2025, scaricabile gratuitamente al presente link https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html*



Le priorità per creare un sistema di governance efficace divengono quindi:

1. La **valutazione dei rischi** – incluse le **minacce cyber** derivanti dall'utilizzo di strumenti informatici basati sull'intelligenza artificiale – effettuata sulla base di standard nazionali, europee e internazionali[8], da professionisti con competenze specifiche in materia

2. La **definizione di procedure aziendali trasparenti e chiare** sull'uso delle soluzioni di intelligenza artificiale da parte dei dipendenti dell'azienda, fondate sul rispetto dell'etica e dei diritti fondamentali della persona quali la riservatezza e la privacy

3. La **conformità alle normative**, in particolare in materia di protezione dei dati personali (GDPR), di cybersecurity (NIS 2 e DORA), e di intelligenza artificiale (AI ACT) anche se questo può avere impatti in termini di aumento dei budget destinati all'area informatica[9]

4. L'aggiornamento costante dell'infrastruttura tecnologica aziendale, attraverso l'adozione di soluzioni informatiche e **misure di sicurezza**[10] sempre più efficaci in termini di loss prevention e disaster recovery

[8] *Per la gestione del rischio dei sistemi di IA (AI risk management), oltre all'art. 29 dell'AI ACT relativo alla Fundamental Rights Impact Assessment, si vedano gli standard internazionali ISO 42001:2023 e 23894:20239*

[9] *Come evidenziato nell'articolo The impact of AI on cybersecurity di McKinsey del 14 novembre 2024 "compliance with the European Union's NIS 2 Directive is expected to increase cyber budgets by up to 22 percent in the first years following its implementation. Already, cyber regulatory risk remediation constitutes an average of more than 10 percent of cyber budgets"*

5. La pianificazione e l'organizzazione della **formazione** per il personale al fine di creare una cultura sui temi cybersecurity e AI e di una formazione specifica per i dipendenti della Funzione ICT, soprattutto in materia di sicurezza cloud e machine learning[11]

6. La **riorganizzazione della governance aziendale** che tenga conto della definizione di ruoli e dell'allocazione di responsabilità ai fini di un monitoraggio costante della infrastruttura IT e Cyber. Tra l'altro, la recente normativa NIS 2 impone di valutare la nomina di un CISO (Chief Information Security Officer).

[10] Sulle misure per la gestione del rischio cyber si veda il regolamento di esecuzione n. 2024/2690 pubblicato in Gazzetta Ufficiale UE il 18 ottobre 2024, di attuazione della Direttiva NIS 2

[11] Vd. figura 4 nell'articolo The impact of AI on cybersecurity, McKinsey, 14 novembre 2024

Per ulteriori informazioni su questo argomento e su Technology Industry Group in Europe and Italy, contattare

Francesco Marconi
EU and Italian Technology Industry Group Coordinator
francesco.marconi@it.andersen.com

You may also be interested in

L'AI nel mondo del lavoro: prospettive, opportunità e aspetti critici
AI Act: entra in vigore il nuovo Regolamento Europeo

ANDERSEN