LEXIA	Data: 7 marzo 2026
Testata: Moneta	

Moneta

Effetto Milano-Cortina, per il cibo made in Italy un export da Olimpiadi

Paolo Falcioni

P.12-13

Azienda in pericolo se l'algoritmo IA resta nascosto dentro il cassetto

Aumenta il numero di dipendenti che utilizza in segreto Chatbot gratuiti non autorizzati. Programmi obsoleti e omessi controlli ampliano la tendenza. Per le imprese possibili ricadute onerose

Chiara Ricciolini

Si fa ma non si dice. Sempre più dipendenti ricorrono a strumenti di intelligenza artificiale estranei all'azienda per svolgere le proprie attività lavorative quotidiane. E lo fanno di nascosto dai datori di lavoro che - forse - il più delle volte fingono di non sapere. Questo accade perché le imprese non hanno ancora integrato l'automazione nei flussi di produzione o, peggio, hanno investito in strumenti obsoleti e meno performanti persino rispetto alle versioni gratuite di ChatGPT, Gemini e Claude. Si tratta del fenomeno dell'intelligenza artificiale ombra: l'uso non autorizzato da parte degli impiegati di qualsiasi applicazione di IA senza l'approvazione aziendale.

Secondo IBM tra il 2023 e il 2024 l'adozione di applicazioni di intelligenza artificiale generativa tra i lavoratori è passata dal 74% al 96%. Si sta diffondendo a macchia d'olio: chi può velocizzare o migliorare le proprie performance deve solo digitare il nome di un qualsiasi chatbot nella barra di ricerca. E lo fa ormai già da qualche anno. Oggi oltre un terzo, il 38%, ammette di condividere informazioni sensibili con un chat-

bot commerciale - generalmente nella versione gratuita - senza il permesso del datore di lavoro. «La Shadow AI è l'utilizzo non autorizzato di strumenti di intelligenza artificiale da parte dei dipendenti - come ChatGPT o Gemini - al di fuori di qualsiasi policy aziendale» spiega a *Moneta* Aurora Agostini, legale partner di Lexia avvocati. «I dipendenti vi ricorrono per migliorare la produttività, velocizzare i processi e aggirare le inefficienze operative, generando un fenomeno tutt'altro che marginale: secondo il report BCG AI at Work 2025, il 54% dei dipendenti dichiara che utilizzerebbe strumenti di IA anche in assenza di autorizzazione aziendale, con una concentrazione significativa tra Gen Z e Millennials, che raggiungono il 62%». E ciò avviene a causa dell'inadeguatezza degli strumenti aziendali messi a disposizione.

PRIVACY

Le sanzioni per violazione della normativa sulla protezione dei dati possono costare caro alle aziende: fino a 20 milioni di euro o il 4% del fatturato globale dell'anno precedente. Senza una supervisione centrale dell'attività dei dipendenti il fenomeno è il veicolo perfetto di gravi vulnerabilità. «Il rischio principale è l'esfiltrazione di dati strategici - codice sorgente, chiavi API, previsioni di budget, informazioni su clienti e dipendenti - che vengono trasmessi a server di terze parti senza cifratura, senza logging e senza garanzie contrattuali di non utilizzo a fini di training dei modelli» prosegue.

COMPETITIVITÀ

Gartner stima che entro il 2030 questi punti ciechi segneranno la linea di demarcazione tra aziende che hanno impiegato l'intelligenza artificiale in modo sicuro e strategico e quelle che sono rimaste impantanate nei vecchi sistemi e sono destinate a esser superate da realtà più lungimiranti. Si calcola che entro il 2030 oltre il 40% delle aziende subirà incidenti di sicurezza legati all'uso di intelligenza artificiale ombra.

Per arginare il fenomeno le imprese devono armarsi di un approccio lucido, scevro da ipocrisie e non detti. Chi fa impresa deve aprire gli occhi e informare il personale sui rischi dell'uso non autorizzato, consolidare una cultura aziendale attenta alla sicurezza e al rispetto delle regole interne. È poi essenziale stabilire linee guida chiare, ricche di criteri, limiti e responsabilità precise.

COMPETENZE

Il problema non è imputabile alla malafede dei dipendenti, ma piuttosto alla pressione sul lavoro unita all'assenza di strumenti efficaci. Il 55% delle imprese in Italia mette in guardia sull'esistenza di una grave carenza di competenze che rende molto difficile l'integrazione delle nuove risorse dell'automazione in un team di lavoro. Dato che costituisce il principale ostacolo per la formulazioni di politiche aziendali omogenee ed efficaci. Ma è un circolo vizioso: è così che i dipendenti sono costretti a rivolgersi in modo scomposto e inconsapevole a soluzioni esterne per far fronte alle scadenze. Sempre secondo IBM, il 13% delle organizzazioni ha registrato violazioni di modelli o applicazioni di intelligenza artificiale, mentre l'8% non è in grado di confermare se siano state compromesse. Tra quelle coinvolte, il 97% dichiara di non avere controlli di accesso basati sull'intelligenza artificiale.

Di conseguenza il 60% degli incidenti legati all'intelligenza artificiale ha comportato la compromissione dei dati e il 31% ha provocato interruzioni operative. Ma le aziende sembrano preferire un'adozione caotica e approssimativa di questi strumenti e spesso non hanno alcuna strategia per farli fruttare al meglio. Non capendo che questo causa dei costi altissimi: i sistemi non monitorati risultano più vulnerabili e, quando subiscono violazioni, generano costi molto elevati. Il 63% delle società che hanno subito violazioni non dispone di regole interne per governare l'uso dell'IA e tra quelle che invece hanno regole formalizzate solo il 34% esegue ve-

rifiche regolari per rilevare l'uso non autorizzato di strumenti di IA.

COSTI

Ecco il costo dell'IA ombra: «Sul piano legale, oltre alle sanzioni GDPR, il quadro si arricchisce con l'AI Act europeo e la Direttiva NIS2, che impongono alle organizzazioni obblighi crescenti di governance tecnologica. La risposta non è vietare l'IA, ma disciplinarla con l'adozione di strumenti aziendali di mitigazione, la definizione di policy chiare sull'uso degli strumenti di AI e la formazione continuativa del personale sui profili di rischio legale e informatico connessi all'uso improprio degli strumenti di intelligenza artificiale» spiega l'esperta. Gli incidenti di sicurezza legati all'IA ombra hanno provocato un aumento di fuga di informazioni riservate nel 65% dei casi e della proprietà intellettuale nel 40%. A rendere tutto ancora più preoccupante c'è che il 16% delle violazioni ha coinvolto aggressori che hanno sfruttato strumenti di intelligenza artificiale per attacchi di phishing e cybercrimine online.

Le sanzioni per violazione delle norme sulla privacy possono costare alle società fino al 4% del fatturato globale annuo

Il 38% degli impiegati ammette di condividere regolarmente informazioni riservate attraverso un assistente virtuale

40%

Le imprese che entro il 2030 subiranno incidenti a causa dell'adozione di agenti conversazionali non validati da parte dei propri assunti

Zero regole molti rischi

LEXIA	Data: 9 marzo 2026
Testata: Moneta	Link

Moneta

IMPRESA E MANAGEMENT

In ufficio con l'algoritmo nascosto nel cassetto, ma quando l'IA è ombra l'azienda è in pericolo

Aumenta il numero di dipendenti che utilizza in segreto chatbot gratuiti non autorizzati. Programmi obsoleti e omessi controlli ampliano la tendenza. Per le imprese possibili conseguenze salate

Chiara Ricciolini

9 Marzo 2026

Si fa ma non si dice. Sempre più dipendenti ricorrono a strumenti di intelligenza artificiale estranei all'azienda per svolgere le proprie attività lavorative quotidiane. E lo fanno di nascosto dai datori di lavoro che – forse – il più

delle volte fingono di non sapere. Questo accade perché le imprese non hanno ancora integrato l'automazione nei flussi di produzione o, peggio, hanno investito in strumenti obsoleti e meno performanti persino rispetto alle versioni gratuite di **ChatGPT, Gemini e Claude**. Si tratta del fenomeno dell'intelligenza artificiale ombra: l'uso non autorizzato da parte degli impiegati di qualsiasi applicazione di IA senza l'approvazione aziendale.

Secondo *IBM* tra il 2023 e il 2024 l'adozione di applicazioni di intelligenza artificiale generativa tra i lavoratori è passata **dal 74% al 96%**. Oggi oltre un terzo, **il 38%**, ammette di condividere informazioni sensibili con un chatbot commerciale – generalmente nella versione gratuita – senza il permesso del datore di lavoro.

«La Shadow AI è l'utilizzo non autorizzato di strumenti di intelligenza artificiale da parte dei dipendenti – come ChatGPT o Gemini – al di fuori di qualsiasi policy aziendale» spiega a Moneta **Aurora Agostin**i, Partner di **Lexia**. «I dipendenti vi ricorrono per migliorare la produttività, velocizzare i processi e aggirare le inefficienze operative, generando un fenomeno tutt'altro che marginale: secondo il report BCG AI at Work 2025, il 54% dei dipendenti dichiara che utilizzerebbe strumenti di IA anche in assenza di autorizzazione aziendale, con una concentrazione significativa tra Gen Z e Millennials, che raggiungono il 62%». E ciò avviene a causa dell'inadeguatezza degli strumenti aziendali messi a disposizione.

Privacy

Le sanzioni per violazione della normativa sulla protezione dei dati possono costare caro alle aziende: fino a 20 milioni di euro o il 4% del fatturato globale dell'anno precedente. Senza una supervisione centrale dell'attività dei dipendenti il fenomeno è il veicolo perfetto di gravi vulnerabilità. «Il rischio principale è l'esfiltrazione di dati strategici – codice sorgente, chiavi API, previsioni di budget, informazioni su clienti e dipendenti – che vengono trasmessi a server di terze parti senza cifratura, senza logging e senza garanzie contrattuali di non utilizzo a fini di training dei modelli» prosegue.

Competitività

Gartner stima che entro il 2030 questi punti ciechi segneranno la

linea di demarcazione tra aziende che hanno impiegato l'intelligenza artificiale in modo sicuro e strategico e quelle che sono rimaste impantanate nei vecchi sistemi e sono destinate a esser superate da realtà più lungimiranti. Si calcola che entro il 2030 oltre il 40% delle aziende subirà incidenti di sicurezza legati all'uso di intelligenza artificiale ombra. Per arginare il fenomeno le imprese devono armarsi di un approccio lucido, scevro da ipocrisie e non detti. Chi fa impresa deve aprire gli occhi e informare il personale sui rischi dell'uso non autorizzato e consolidare una cultura aziendale attenta alla sicurezza e al rispetto delle regole interne. È poi essenziale stabilire linee guida chiare, ricche di criteri, limiti e responsabilità precise.

Competenze

Il problema non è imputabile alla malafede dei dipendenti, ma piuttosto alla pressione sul lavoro unita all'assenza di strumenti efficaci. **Il 55% delle imprese in Italia mette in guardia sull'esistenza di una grave carenza di competenze che rende molto difficile l'integrazione delle nuove risorse dell'automazione in un team di lavoro**. Dato che costituisce il principale ostacolo per la formulazioni di politiche aziendali omogenee. Per questo motivo i dipendenti sono costretti a rivolgersi in modo scomposto e inconsapevole a soluzioni esterne per far fronte alle scadenze. Sempre secondo IBM, il 13% delle organizzazioni ha registrato violazioni di modelli o applicazioni di intelligenza artificiale, mentre l'8% non è in grado di confermare se siano state compromesse. Tra quelle coinvolte, il 97% dichiara di non avere controlli di accesso basati sull'intelligenza artificiale.

Di conseguenza il 60% degli incidenti legati all'intelligenza artificiale ha comportato la compromissione dei dati e il 31% ha provocato interruzioni operative. Ma le aziende sembrano preferire un'adozione caotica e approssimativa di questi strumenti e non hanno nessuna strategia per farli fruttare al meglio. Non capendo che questo causa dei costi altissimi: i sistemi non monitorati risultano più vulnerabili e, quando subiscono violazioni, generano costi molto elevati. Il 63% delle società che hanno subito violazioni non dispone di regole interne per governare l'uso dell'IA e tra quelle che invece hanno regole formalizzate solo il 34% esegue verifiche regolari per rilevare l'uso non autorizzato di strumenti di IA.

Costi

Ecco il costo dell'IA ombra: «Sul piano legale, oltre alle sanzioni GDPR, il quadro si arricchisce con l'AI Act europeo e la Direttiva

NIS2, che impongono alle organizzazioni obblighi crescenti di governance tecnologica. La risposta non è vietare l'IA, ma disciplinarla con l'adozione di strumenti aziendali di mitigazione, la definizione di policy chiare sull'uso degli strumenti di AI e la formazione continuativa del personale sui profili di rischio legale e informatico connessi all'uso improprio degli strumenti di intelligenza artificiale» spiega l'esperta. Gli incidenti di sicurezza legati all'IA ombra hanno provocato un aumento di fuga di informazioni riservate nel 65% dei casi e della proprietà intellettuale nel 40%. A rendere tutto ancora più preoccupante c'è che il 16% delle violazioni ha coinvolto aggressori che hanno sfruttato strumenti di intelligenza artificiale per attacchi di phishing e cybercrimine online.

Valletta
PR ADVISORY

LEXIA
LAW | TAX | INNOVATION

Rassegna Stampa