

Come l'intelligenza artificiale ricostruisce il know-how delle imprese e ridisegna i confini della sovranità

Serie Sovranità Tecnologica / 06

Serie Sovranità Tecnologica

Documento di analisi strategica,
ottobre 2026

Con il contributo di

Franco Bernabè

Ceo TechVisory

Antonio Dina

Executive Editor Rivista.AI

Fabio Ricceri

Executive Editor Rivista.AI

Rivista.AI

mail: redazione@rivista.ai

newsletter: rivistaai.substack.com

web: www.rivista.ai

L'effetto mosaico. Come l'intelligenza artificiale ricostruisce il know-how delle imprese e ridisegna i confini della sovranità industriale

Sommario

Premessa. La conoscenza non è mai un dato neutrale
Pag. **3**

Executive Summary. Due livelli dello stesso problema
Pag. **4**

Il capitale invisibile delle imprese
Pag. **6**

Come si forma, nel tempo, questo patrimonio
Pag. **8**

Come l'AI può ricomporre il patrimonio invisibile
Pag. **9**

Quando il mosaico esce dalla teoria
Pag. **11**

Dove va davvero quel patrimonio quando esce
dai confini aziendali
Pag. **13**

Quando la conoscenza altera gli equilibri della
concorrenza
Pag. **15**

Cosa significa "sovranità" nell'intelligenza artificiale
Pag. **17**

Cosa si può fare davvero
Pag. **19**

Conclusioni. La sovranità comincia da un prompt
Pag. **21**

Premessa.

La conoscenza non è mai un dato neutrale

Ogni grande trasformazione tecnologica porta con sé una promessa di efficienza e, quasi sempre, una sottovalutazione iniziale del prezzo che quella efficienza comporta. Con Internet abbiamo imparato che ciò che sembrava gratuito veniva spesso pagato in un'altra moneta: i dati, le preferenze, le relazioni, i comportamenti. I servizi di posta elettronica hanno analizzato per anni il contenuto delle comunicazioni per automatizzare funzioni e, in alcuni casi, alimentare sistemi pubblicitari; le piattaforme social hanno costruito una parte rilevante del proprio vantaggio competitivo sulla capacità di osservare, classificare e trasformare le interazioni degli utenti in informazione economicamente utilizzabile.

Non c'è quindi particolare ragione per affrontare l'intelligenza artificiale con maggiore ingenuità. Sebbene le aziende che sviluppano i grandi modelli assicurino oggi, soprattutto nei servizi professionali ed enterprise, livelli di protezione dei dati molto più rigorosi e dichiarino in molti casi di non utilizzare le informazioni dei clienti per addestrare i propri modelli, sarebbe un errore ridurre la questione alla sola domanda se una determinata conversazione venga o meno utilizzata per il training.

Il problema è più ampio. Ogni tecnologia impara anche dal mercato nel quale viene utilizzata: dai problemi che è chiamata a risolvere, dai casi d'uso che emergono, dalle integrazioni che vengono richieste, dagli errori che vengono

segnalati e, soprattutto, dalla progressiva comprensione dei processi nei quali diventa indispensabile. È così che un prodotto diventa un'infrastruttura e che un'infrastruttura può trasformarsi in una dipendenza.

Per l'Europa e per l'Italia questa dinamica assume una rilevanza particolare. Disponiamo di una straordinaria quantità di conoscenza industriale, scientifica e professionale, gran parte della quale non è contenuta nei brevetti o nei manuali. Vive nelle aziende, nelle competenze delle persone, nelle procedure costruite attraverso l'esperienza, negli errori che si è imparato a non ripetere.

L'intelligenza artificiale cambia questa condizione perché, per essere utile, deve essere messa nelle condizioni di comprendere il contesto. E per farle comprendere il contesto siamo noi a doverglielo raccontare.

È qui che l'"effetto mosaico" descritto in questo Paper diventa interessante. Il rischio non è necessariamente la sottrazione di un documento riservato o di un segreto industriale. Può essere qualcosa di molto meno visibile: la progressiva trasformazione di frammenti di esperienza in informazioni digitalmente elaborabili. Presi singolarmente significano poco. Messi insieme possono raccontare molto.

Franco Bernabè
Presidente TechVisory

Executive Summary

Due livelli dello stesso problema

Nel 2023 Samsung si trovò di fronte a un problema che molte imprese avrebbero presto imparato a conoscere. Alcuni dipendenti della divisione semiconduttori avevano utilizzato ChatGPT per lavorare più velocemente: un ingegnere aveva inserito codice sorgente riservato per correggere un errore, un altro aveva condiviso informazioni tecniche relative ai processi produttivi, un terzo aveva caricato la trascrizione di una riunione interna per ottenere un verbale. Non si trattava di un attacco informatico né di un furto di dati. Erano dipendenti che cercavano semplicemente di fare meglio e più rapidamente il proprio lavoro, non certo di divulgare informazioni sensibili.

Samsung reagì limitando e successivamente vietando l'utilizzo degli strumenti di intelligenza artificiale generativa sui dispositivi aziendali.

Il caso anticipava una questione destinata a diventare molto più grande: che cosa accade quando, per ottenere valore dall'intelligenza artificiale, cominciamo a raccontarle come funzionano le nostre aziende?

Una parte importante del patrimonio competitivo di un'impresa non è contenuta nei brevetti, nei marchi o nei documenti classificati come riservati. Vive nell'esperienza delle persone, nelle procedure sviluppate nel tempo, nelle eccezioni alle regole, negli errori che si è imparato a evitare, nelle relazioni con clienti e fornitori, nelle soluzioni trovate a problemi che altri non hanno ancora incontrato.

È conoscenza dispersa e spesso tacita, particolarmente importante nel sistema industriale italiano, dove il vantaggio competitivo di molte imprese coincide proprio con un saper fare accumulato nel corso degli anni.

L'intelligenza artificiale generativa modifica questa condizione perché, per essere davvero utile, ha bisogno di contesto. E quel contesto siamo noi a fornirglielo: attraverso domande, documenti, correzioni, spiegazioni, codice, analisi e descrizioni dei problemi che vogliamo risolvere.

È qui che nasce ciò che in questo Paper chiamiamo effetto mosaico. Attraverso minuscole tessere di informazione, apparentemente innocue se osservate una per una, l'intelligenza artificiale può contribuire a comporre un affresco molto più ampio: processi, competenze, problemi, eccezioni e soluzioni che costituiscono una parte del sapere più intimo dell'azienda. Una singola domanda racconta poco. Centinaia o migliaia di interazioni possono raccontare molto di più.

Questo non significa che ogni informazione inserita in un sistema di AI venga automaticamente utilizzata per addestrare un modello. Training, utilizzo del servizio, memoria delle conversazioni, feedback e trattamento dei dati sono processi differenti e dipendono dal prodotto, dalle configurazioni e dalle condizioni contrattuali. Ma il valore può

emergere anche dai casi d'uso, dalle integrazioni, dai problemi reali che vengono sottoposti ai sistemi e dalla progressiva centralità che quelle piattaforme acquistano nei processi aziendali.

Osservato da lontano, lo stesso fenomeno assume una dimensione strategica. L'Europa produce una quantità straordinaria di conoscenza industriale, scientifica e professionale, mentre una parte crescente delle infrastrutture attraverso cui questa conoscenza viene elaborata appartiene a operatori extraeuropei. La protezione del know-how della singola impresa e la sovranità tecnologica europea diventano così due livelli dello stesso problema.

La risposta, tuttavia, non è rinunciare all'intelligenza artificiale né immaginare un'improbabile autarchia tecnologica. È imparare a utilizzarla sapendo che non tutte le informazioni, non tutti i processi e non tutti gli strumenti devono essere trattati allo stesso modo.

Questo Paper propone quindi alcune scelte concrete: classificare il patrimonio informativo prima di affidarlo all'AI; distinguere tra strumenti consumer, servizi enterprise e ambienti realmente controllati; utilizzare soluzioni locali o on-premise quando il valore del know-how lo richiede; verificare chiamate e flussi verso servizi esterni; separare gli ambienti di sperimentazione dai sistemi critici; controllare accessi e condizioni contrattuali; formare le persone affinché riconoscano non soltanto il dato riservato, ma anche il valore che può emergere dalla combinazione di informazioni apparentemente innocue.

Perché il punto non è costruire un recinto intorno alla conoscenza. Un patrimonio che non circola, non viene utilizzato e non incontra

nuove tecnologie rischia a sua volta di perdere valore.

La questione è mantenere la capacità di decidere quale conoscenza può uscire dall'organizzazione, attraverso quale infrastruttura, per quale finalità e a quali condizioni.

Da vicino è la decisione di un dipendente davanti a una finestra di chat.

Da lontano è la decisione di un sistema industriale su chi possa trasformare la sua conoscenza in capacità tecnologica e valore economico.



Il capitale invisibile delle imprese

Come si forma il sapere invisibile dell'impresa

Quando un'azienda pensa a come proteggere ciò che sa fare meglio dei concorrenti, il primo riflesso è quasi sempre giuridico: un brevetto, un marchio registrato, una clausola di riservatezza, un accordo di non concorrenza.

Sono strumenti utili, ma coprono una parte molto più piccola di quanto si creda del vero patrimonio di conoscenza di un'organizzazione. Sono protette da un brevetto le invenzioni che soddisfano requisiti specifici e per le quali l'impresa ha scelto di chiedere una tutela.

Sono protetti dal marchio i segni distintivi con cui l'azienda si presenta sul mercato. Contratti e clausole di riservatezza possono disciplinare l'utilizzo e la divulgazione delle informazioni alle quali si applicano.

Anche il know-how può essere tutelato come segreto commerciale, purché abbia valore proprio perché segreto e l'impresa abbia adottato misure ragionevoli per mantenerlo tale.

Ma una parte molto più ampia della conoscenza aziendale non si presenta in nessuna di queste forme: è il modo in cui un tecnico riconosce, da un rumore anomalo, che un macchinario sta per guastarsi; sono le ragioni non scritte per cui un cliente viene gestito in un certo modo; gli aggiustamenti empirici che un reparto produttivo ha introdotto rispetto alla procedura ufficiale; la combinazione di fornitori e piccoli compromessi che permette di rispettare una consegna quando qualcosa va storto; l'insieme degli errori commessi in passato e delle correzioni che ne sono seguite. Si tratta, in tutti questi casi, di conoscenza a tutti gli effetti.

E spesso è proprio quella che distingue due imprese che sulla carta dispongono delle stesse tecnologie, acquistano gli stessi macchinari e operano nello stesso mercato.

Gli studiosi delle organizzazioni la definiscono spesso conoscenza tacita, per distinguerla da quella esplicita e documentata. Non è necessariamente segreta e non è necessariamente priva di protezione giuridica. Più semplicemente, una parte rilevante di questo sapere non è mai stata organizzata pensando che dovesse essere protetta come un brevetto o custodita come un documento riservato.

Soprattutto, questo patrimonio non nasce in un momento preciso: si forma nel tempo.

Si forma attraverso l'esperienza diretta, ogni volta che un'azienda incontra un problema e trova un modo per risolverlo. La soluzione può non entrare mai in una procedura ufficiale, ma modifica il comportamento di chi lavora e viene trasmessa attraverso l'osservazione, il confronto e la pratica.

Si forma attraverso gli errori. Un lotto difettoso, una previsione sbagliata, un progetto che ha richiesto più tempo del previsto lasciano dietro di sé lezioni che raramente vengono formalizzate per intero, ma cambiano il modo in cui l'organizzazione affronta la volta successiva lo stesso problema.

Si forma attraverso le relazioni. Il rapporto con un fornitore storico, la sensibilità verso le esigenze non dichiarate di un cliente importante, la capacità di capire quando insistere e quando fermarsi in una trattativa sono conoscenza tanto quanto una procedura tecnica, anche se non contenute in un database.

Si forma attraverso la selezione delle pratiche migliori. Tra le molte varianti con cui persone diverse affrontano lo stesso compito, alcune

funzionano meglio e progressivamente si diffondono, mentre altre vengono abbandonate.

L'organizzazione accumula così migliaia di micro ottimizzazioni che nessuno ha progettato nel loro insieme.

E si forma attraverso la cultura. Dopo anni, errori, esperienza, relazioni e pratiche diventano un modo condiviso di interpretare i problemi, stabilire le priorità e riconoscere ciò che funziona. È probabilmente la componente più difficile da misurare e, proprio per questo, una delle più difficili da imitare.

Per molto tempo questa caratteristica ha costituito anche una forma implicita di protezione. La conoscenza tacita è difficile da trasferire perché è dispersa tra persone, esperienze, relazioni e contesti. Un concorrente può acquistare la stessa macchina, assumere un tecnico, studiare un prodotto o analizzare un processo, ma non può necessariamente replicare in un solo gesto ciò che un'organizzazione ha imparato in dieci, venti o cinquant'anni.

Ciò che può essere trasferito in pochi secondi può aver richiesto decenni per essere costruito

È una considerazione particolarmente importante per il sistema industriale italiano.

In molti settori nei quali il Made in Italy ha costruito il proprio vantaggio competitivo, dalla moda all'agroalimentare, dalla meccanica di precisione alla farmaceutica, il valore non risiede soltanto nella materia prima, nella macchina utilizzata o nella proprietà intellettuale formalmente registrata.

Sta anche nel modo in cui generazioni di persone hanno affinato un gesto, modificato un processo, riconosciuto un'eccezione, costruito una relazione o trovato una soluzione.

Il patrimonio dell'impresa è quindi molto più grande dell'insieme delle informazioni che essa considera riservate.

E il problema posto dall'intelligenza artificiale nasce proprio qui.

Perché per utilizzare un assistente generativo non è necessario consegnargli l'intero patrimonio aziendale: è sufficiente spiegargli, ogni volta, il pezzo di contesto necessario per risolvere il problema che abbiamo davanti.

Una procedura da migliorare. Un'anomalia da interpretare. Una trattativa da preparare. Un documento da correggere. Una decisione da confrontare con quelle prese in passato.

Nessuna di queste informazioni, da sola, può necessariamente rappresentare un segreto industriale. Ma una parte di quella conoscenza che per decenni è rimasta dispersa nelle persone e nei processi comincia così a essere trasformata in testo, documenti e conversazioni digitali.

Un episodio recente aiuta forse a comprendere meglio quanto questo patrimonio abbia già acquistato un valore autonomo nell'economia dell'intelligenza artificiale.

Nell'agosto 2026 Google ha offerto 10 milioni di dollari per acquistare, nell'ambito della procedura fallimentare di Spirit Airlines, una parte dei dati interni accumulati dalla compagnia nel corso della propria attività: email dei dipendenti, messaggi scambiati su Microsoft Teams, calendari, fogli di calcolo e informazioni relative alle attività operative, al marketing e alla produttività.

Google ha dichiarato di voler utilizzare quel patrimonio, una volta rimosse le informazioni personali identificabili, anche per lo sviluppo e l'addestramento dei propri modelli di AI.

Peraltro l'azienda di Mountain View non era l'unica interessata. Mercor, società specializzata nella produzione di dati per l'addestramento dell'AI, aveva presentato un'offerta da 7,5 milioni di dollari; successivamente Micro1, una startup che lavora anch'essa sui dati destinati ai sistemi di intelligenza artificiale, ha cercato di rilanciare con 12,5 milioni.

È difficile trovare un'immagine più concreta del valore che sta assumendo la conoscenza aziendale accumulata nel tempo.

Ciò che resta di un'impresa non è soltanto il marchio, un brevetto, gli aerei, gli immobili o le attrezzature. Possono avere valore anche anni di email, conversazioni, fogli di calcolo, decisioni operative e documenti di lavoro: la traccia digitale di come un'organizzazione reale ha affrontato problemi reali.

Per un sistema di intelligenza artificiale, proprio questa può essere una materia prima particolarmente preziosa, perché l'insieme racconta come funziona davvero un'azienda.

Ed è a questo punto che la domanda cambia.

Non dobbiamo più chiederci soltanto che cosa stiamo consegnando a un sistema di intelligenza artificiale, ma che cosa quel sistema potrebbe arrivare a comprendere mettendo insieme ciò che gli raccontiamo nel tempo.



Come l'AI può ricomporre il patrimonio invisibile

Il rischio più interessante posto dall'intelligenza artificiale alla conoscenza aziendale non coincide necessariamente con il gesto più evidente: un dipendente che copia deliberatamente un documento riservato all'interno di una chat.

Può nascere in modo molto più ordinario, mentre persone diverse utilizzano un assistente per svolgere meglio attività che fanno parte del loro lavoro quotidiano.

Un dipendente dell'ufficio acquisti chiede aiuto per riformulare un'email a un fornitore e, per ottenere una risposta utile, specifica tempi di consegna, condizioni di pagamento e ragioni per cui quella fornitura è particolarmente importante. Un tecnico di produzione sottopone un problema relativo a una macchina, descrivendo la sequenza di lavorazione, l'anomalia osservata e le correzioni già tentate. Un responsabile commerciale prepara una trattativa e indica caratteristiche del cliente, margini disponibili, soglie di sconto e precedenti negoziali.

Nessuna di queste richieste, considerata isolatamente, deve necessariamente contenere un segreto industriale. Ognuna può apparire “come una normale richiesta di supporto.

Il significato cambia quando le tessere cominciano a comporre un mosaico

È questo il punto che distingue l'intelligenza artificiale generativa da molti degli strumenti digitali utilizzati in precedenza. Per ottenere una risposta pertinente, l'utente è incentivato a fornire contesto: spiegare il problema, descrivere le eccezioni, precisare ciò che è già stato tentato, indicare vincoli e obiettivi.

Più il sistema è utile in una situazione specifica, più deve conoscere ciò che rende quella situazione specifica. Ed è spesso proprio in quel contesto che si trova una parte del know-how dell'impresa.

Un singolo scambio può dire poco, ma una

successione di interazioni può contenere informazioni sui fornitori, sui processi produttivi, sulle logiche commerciali, sulle procedure interne, sui problemi ricorrenti e sulle soluzioni che hanno funzionato. Se poi persone che appartengono a funzioni diverse descrivono parti differenti della stessa organizzazione, le tessere disponibili aumentano ulteriormente.

Attraverso minuscole tessere di informazione, apparentemente insignificanti se osservate separatamente, l'intelligenza artificiale può contribuire a comporre un grande affresco dei processi, delle competenze e persino dei segreti più intimi di un'azienda.

È quello che chiamiamo effetto mosaico: il valore informativo che emerge dalla combinazione e dalla contestualizzazione di frammenti che, presi singolarmente, possono sembrare innocui o scarsamente significativi.

Questo non significa che qualsiasi assistente di intelligenza artificiale costruisca automaticamente un dossier sull'azienda che lo utilizza. Il modo in cui le interazioni vengono conservate, associate a un account, rese disponibili alla memoria del sistema, utilizzate per migliorare il servizio o eventualmente impiegate per l'addestramento dipende dal prodotto, dalle configurazioni adottate e dalle condizioni contrattuali.

Servizi consumer, piattaforme enterprise, API e sistemi installati in ambienti controllati possono offrire garanzie molto differenti.

La distinzione è fondamentale, ma non elimina il problema, semmai lo rende più preciso. Perché la sicurezza informativa è stata tradizionalmente costruita soprattutto intorno alla sensibilità del singolo dato: questo documento è riservato? Questa informazione può uscire dall'azienda? Questo file contiene dati personali? Questo codice è proprietario?

L'effetto mosaico introduce una domanda

diversa: che cosa diventa conoscibile quando informazioni che singolarmente possiamo considerare innocue vengono messe in relazione tra loro?

Un nome di fornitore può non essere sensibile. Un tempo medio di consegna può non esserlo. Una soglia di prezzo, una modifica apportata a una procedura⁴, il motivo per cui una determinata soluzione non funziona o la descrizione di un problema incontrato con un cliente possono non esserlo.

Ma la loro combinazione può raccontare molto più di ciascuna informazione presa separatamente. Ed è qui che il problema diventa anche organizzativo. L'azienda può controllare relativamente bene un documento classificato come riservato; è molto più difficile controllare centinaia di microdecisioni prese ogni giorno da persone che non hanno la percezione di stare condividendo qualcosa di strategico.

Il dipendente non pensa necessariamente di stare trasferendo know-how aziendale. Pensa: "sto cercando di farmi aiutare a risolvere un problema.

È proprio questa normalità a rendere il fenomeno difficile da governare. Non serve immaginare un comportamento scorretto, una violazione deliberata delle policy o un attacco informatico.

È sufficiente che uno strumento diventi abbastanza utile da entrare nel lavoro quotidiano e che, per ottenere risultati migliori, gli utenti imparino progressivamente a fornirgli più contesto.

Si crea così un paradosso: più l'assistente conosce il contesto dell'impresa, più può diventare utile. Ma una parte di ciò che lo rende utile coincide precisamente con ciò che rende quell'impresa diversa dalle altre e proprio per questo il problema non può essere

affrontato soltanto stabilendo un elenco di informazioni che è vietato inserire in un chatbot.

Una classificazione dei dati rimane necessaria, ma occorre affiancarle una consapevolezza diversa: il valore di un'informazione non dipende soltanto da ciò che rivela da sola, ma

anche da ciò che può contribuire a rivelare quando questa viene combinata con altre informazioni.

Una domanda non racconta un'azienda. Un mosaico di domande può raccontare molto di più.

Quando il mosaico esce dalla teoria

Dalla prima fuga di codice alla Shadow AI: che cosa è successo quando l'intelligenza artificiale è entrata nel lavoro quotidiano

L'effetto mosaico descrive un rischio che per sua natura è difficile da osservare: nessuno vede il mosaico mentre vengono posate le singole tessere. Ma negli ultimi anni sono emersi un certo numero di episodi da mostrare che il passaggio di informazioni aziendali attraverso strumenti di intelligenza artificiale non è più soltanto un'ipotesi teorica.

Il caso che ha reso evidente il problema risale al 2023. Samsung scoprì che alcuni dipendenti avevano caricato codice aziendale sensibile su ChatGPT. La reazione fu drastica: in una delle principali divisioni venne vietato l'utilizzo di strumenti di intelligenza artificiale generativa esterni. Nel memo interno riportato da Bloomberg, l'azienda spiegava di essere preoccupata anche dal fatto che le informazioni inviate a servizi come ChatGPT, Bard e Bing venissero elaborate su server esterni, rendendone difficile il recupero o la cancellazione.

Il punto interessante non è soltanto che qualcuno abbia commesso un errore. È il modo in cui l'errore è avvenuto. Non attraverso un attacco informatico, una chiavetta USB sottratta o l'invio deliberato di un documento a un concorrente, ma utilizzando uno strumento che prometteva di rendere più semplice il lavoro.

Samsung non era sola. Già nel gennaio dello stesso anno Amazon aveva avvertito i dipendenti di non inserire in ChatGPT informazioni confidenziali, compreso il codice sul quale stavano lavorando. Nel febbraio JPMorgan aveva limitato l'accesso al servizio nell'ambito dei propri controlli sul software di terze parti. A maggio Apple impose restrizioni sull'utilizzo di ChatGPT e di altri strumenti esterni per il timore che potessero essere condivise informazioni confidenziali. Un mese dopo persino Google avvertì i propri dipendenti di non inserire materiale riservato nei chatbot, compreso il proprio Bard.

Dal caso individuale alla Shadow AI

Nel secondo trimestre del 2025 Harmonic Security ha analizzato un campione di un milione di prompt e 20.000 file inviati da lavoratori di aziende statunitensi e britanniche a più di 300 strumenti GenAI e applicazioni SaaS dotate di funzionalità AI. Il risultato rende bene la dimensione del fenomeno:

- il 4,37% dei prompt conteneva informazioni sensibili;
- il 21,86% dei file caricati conteneva informazioni sensibili.

Nel campione rientravano codice sorgente, credenziali di accesso, algoritmi proprietari, documentazione relativa a fusioni e acquisizioni, dati di clienti e dipendenti e informazioni finanziarie interne. Nello stesso trimestre, l'impresa media osservata da Harmonic aveva visto comparire 23 nuovi strumenti GenAI precedentemente sconosciuti ai propri sistemi di controllo.

Il dato non può essere esteso automaticamente all'intero universo delle imprese: descrive le organizzazioni e le interazioni osservate da Harmonic. Ma mostra qualcosa di altrettanto importante. Il problema non è più soltanto quale chatbot l'azienda abbia deciso ufficialmente di adottare. È quanti strumenti dotati di AI vengono utilizzati all'interno dell'organizzazione senza che l'organizzazione ne abbia necessariamente piena visibilità.

È ciò che viene ormai definito Shadow AI: l'utilizzo di strumenti, account personali o funzionalità AI incorporate in applicazioni SaaS al di fuori o ai margini dei sistemi approvati e controllati dall'impresa. E se l'effetto mosaico nasce dalla combinazione di molti piccoli frammenti, la Shadow AI moltiplica sia il numero delle tessere sia i luoghi nei quali possono finire.

Quando il problema non è il training

C'è infine un terzo livello, che spesso scompare quando la discussione viene ridotta alla domanda: i miei dati vengono utilizzati per addestrare il modello? Nel gennaio 2025, i ricercatori di Wiz scoprirono un database ClickHouse di DeepSeek accessibile pubblicamente e senza autenticazione. Conteneva oltre un milione di righe di log, comprese cronologie delle conversazioni, secret keys e informazioni tecniche sul funzionamento del servizio. Dopo essere stata informata, DeepSeek mise rapidamente in sicurezza il database. Si tratta di un incidente molto diverso dall'errore del dipendente Samsung ma proprio per questo altrettanto importante. Una volta che l'informazione ha attraversato il perimetro dell'impresa, il problema non riguarda soltanto ciò che il modello può imparare ma anche dove quell'informazione viene elaborata, per quanto tempo viene conservata, chi può accedervi, quali sistemi la proteggono e quanto controllo l'impresa conserva realmente sul suo ciclo di vita.



Dove va davvero quel patrimonio quando esce dai confini aziendali

Fin qui abbiamo osservato il fenomeno dal punto di vista dell'impresa. Abbiamo visto come si forma il suo patrimonio invisibile, come può essere progressivamente trasformato in informazione digitale e come l'utilizzo quotidiano dell'intelligenza artificiale moltiplichi i punti attraverso i quali frammenti di quel patrimonio possono attraversare il perimetro aziendale.

La domanda successiva a questo punto è inevitabile: una volta usciti, dove vanno quei frammenti e quale valore possono generare?

La risposta è meno semplice di quanto possa sembrare, perché non esiste un unico canale attraverso il quale la conoscenza europea alimenta l'economia dell'intelligenza artificiale.

E soprattutto non tutto ciò che viene affidato a un sistema AI viene automaticamente utilizzato per addestrare il modello.

È una distinzione importante. Servizi consumer, prodotti enterprise, API e sistemi installati in ambienti controllati possono avere condizioni molto differenti. Alcuni fornitori prevedono l'utilizzo delle conversazioni consumer per migliorare i propri modelli, salvo configurazioni o opt-out; molti servizi enterprise e API dichiarano invece di non utilizzare per il training i dati dei clienti per impostazione predefinita.

Ridurre tutto alla domanda «il mio prompt viene usato per addestrare il modello?», rischia però di far perdere di vista il fenomeno più ampio.

I canali attraverso cui la conoscenza diventa valore

Il primo è l'utilizzo quotidiano degli strumenti conversazionali. Milioni di persone affidano ogni giorno a questi sistemi domande, documenti, problemi, correzioni e contesti professionali. Il trattamento di queste informazioni dipende dal servizio utilizzato e dalle relative condizioni, ma il risultato economico più evidente esiste comunque: l'utilizzo genera ricavi, diffusione, conoscenza dei casi d'uso e integrazione degli strumenti nei processi di lavoro.

Il secondo è l'addestramento sui contenuti disponibili online. I grandi modelli sono stati costruiti utilizzando enormi quantità di testi, codice, immagini e altri materiali provenienti da fonti differenti, compresa una parte del web pubblico. Dentro questo patrimonio si trovano anche articoli, libri, ricerca scientifica, documentazione tecnica, software e contenuti culturali e professionali prodotti in Europa.

Il fatto che un contenuto sia accessibile pubblicamente non significa naturalmente che sia privo di diritti né che il suo utilizzo sia giuridicamente indistinto: proprio intorno a questo confine si sta sviluppando una parte rilevante del confronto tra sviluppatori di AI, titolari dei diritti e regolatori.

Il terzo canale è costituito dai feedback e dalle valutazioni. Un utente può segnalare una risposta sbagliata, preferirne una rispetto ad un'altra, fornire una correzione o partecipare esplicitamente a programmi attraverso i quali determinate interazioni vengono utilizzate per migliorare i sistemi.

Anche qui non esiste un automatismo per cui ogni correzione diventa training. Ma feedback, valutazioni ed esempi di utilizzo reale rappresentano una risorsa importante per comprendere dove i sistemi funzionano, dove falliscono e come possano essere migliorati.

Il quarto canale è quello delle integrazioni aziendali. Quando un assistente entra nei processi di un'impresa, il valore prodotto per il fornitore non dipende necessariamente dall'accesso ai dati del cliente.

Deriva anche dalla diffusione della piattaforma, dalle integrazioni sviluppate, dai problemi che il prodotto impara a risolvere come servizio, dall'ecosistema di software che gli cresce intorno e dalla progressiva difficoltà di sostituirlo una volta che diventa parte del modo di lavorare dell'organizzazione.

Infine esistono gli accordi commerciali sui contenuti, attraverso i quali editori, archivi, piattaforme e altri titolari mettono a disposizione materiali in modo esplicito, regolato e remunerato. In questo caso il trasferimento non è inconsapevole: la conoscenza acquista direttamente un prezzo.

È la stessa logica che abbiamo incontrato, in una forma ancora più sorprendente, nel caso Spirit Airlines: persino email, messaggi, fogli di calcolo e documentazione operativa accumulati durante la vita di un'impresa possono diventare un asset per chi sviluppa sistemi di intelligenza artificiale.

Perché i dati continuano a contare

Dire che i dati sono importanti per l'intelligenza artificiale non significa sostenere che basti accumularne quantità sempre maggiori. Le prestazioni dei sistemi dipendono dall'architettura dei modelli, dalla capacità

di calcolo, dalla qualità e composizione dei dataset, dalle tecniche di post-training, dalle valutazioni, dai dati sintetici e da molti altri fattori.

Ma la qualità dell'informazione continua a essere decisiva. Un manuale tecnico scritto da chi conosce realmente un processo può avere un valore diverso da migliaia di pagine generiche sullo stesso argomento. La descrizione di un guasto da parte di chi lo ha affrontato contiene informazioni diverse da quelle presenti nella scheda tecnica della macchina. Il racconto di una trattativa reale può mostrare sfumature che nessun manuale commerciale riesce a codificare.

È per questo che la conoscenza industriale e professionale europea può essere considerata una forma di materia prima informativa. Non soltanto perché può, in determinate condizioni, entrare nei dataset utilizzati per sviluppare o migliorare i modelli, ma perché alimenta casi d'uso, valutazioni, applicazioni, integrazioni e mercati.

Questo non vuol dire che ogni prompt europeo finisca direttamente e automaticamente nell'addestramento di un modello americano o cinese. Sarebbe una rappresentazione tecnicamente sbagliata.

Il fenomeno è più articolato e, proprio per questo, più interessante. L'Europa è uno dei luoghi in cui vengono prodotte conoscenza scientifica, industriale, professionale e culturale di grande valore. La conoscenza prodotta da imprese, professionisti, ricercatori e cittadini può contribuire in modi diversi alla costruzione di ecosistemi tecnologici il cui controllo e la cui capacità di catturare valore economico si trovano prevalentemente altrove.

Ed è qui che una questione apparentemente informativa diventa competitiva.

Quando la conoscenza altera gli equilibri della concorrenza

Il livello aziendale: rafforzare, senza saperlo, il proprio concorrente

Torniamo alla singola impresa. Se un'azienda italiana utilizza diffusamente strumenti di intelligenza artificiale sviluppati all'esterno del proprio perimetro, non ne consegue automaticamente che stia “addestrando il concorrente”. Sarebbe una semplificazione eccessiva.

Può però accadere qualcosa di più sottile e, proprio per questo, più pericoloso.

L'impresa affida una parte crescente dei propri processi a un'infrastruttura che non controlla direttamente; costruisce integrazioni intorno a quella tecnologia; forma le proprie persone a utilizzarla; adatta progressivamente procedure e flussi di lavoro alle sue caratteristiche.

In alcuni servizi e a determinate condizioni, interazioni e feedback possono inoltre contribuire al miglioramento dei sistemi.

Il risultato è un paradosso competitivo: uno strumento adottato per aumentare la produttività dell'impresa può contemporaneamente rafforzare l'ecosistema tecnologico dal quale l'impresa diventa sempre più dipendente.

Questo non significa che non debba essere utilizzato. Il beneficio di produttività può essere molto superiore al rischio e rinunciare a una tecnologia competitiva può essere, a sua volta, una scelta economicamente dannosa.

La domanda è un'altra: quanto valore vogliamo ottenere da una tecnologia esterna e quanta dipendenza siamo disposti a costruire per ottenerlo?

Il livello europeo: chi produce la conoscenza e chi cattura il valore

Allargando l'inquadratura, la stessa domanda cambia scala. L'Europa dispone di una grande base industriale, università e centri di ricerca, professionisti altamente qualificati, produzione scientifica e culturale e una rete di piccole e medie imprese ricche di know-how specialistico.

Dispone, cioè, di una quantità straordinaria di conoscenza. Ma possedere la conoscenza non equivale necessariamente a controllare l'infrastruttura attraverso cui quella conoscenza viene trasformata in prodotti, servizi e valore economico.

Se una parte crescente dell'attività digitale europea viene mediata da modelli, cloud, piattaforme e infrastrutture sviluppati da operatori extraeuropei, può emergere un'asimmetria: l'Europa produce una parte della materia prima informativa e della domanda, mentre una quota rilevante del valore economico generato dall'infrastruttura che la elabora viene catturata altrove.

Non è una dinamica esclusiva dell'intelligenza artificiale

L'Europa l'ha già sperimentata nei motori di ricerca, nei social network, nel cloud e nelle grandi piattaforme digitali.

Con l'intelligenza artificiale, tuttavia, entra in gioco un elemento ulteriore: queste piattaforme non si limitano a distribuire informazione o mettere in contatto domanda e offerta.

Entrano progressivamente nei processi attraverso i quali la conoscenza viene prodotta, organizzata e utilizzata.

La questione assume una rilevanza ancora maggiore nei settori critici. Energia, sanità, finanza, pubblica amministrazione, industria avanzata e difesa non acquistano soltanto software: possono costruire processi essenziali intorno a infrastrutture la cui evoluzione tecnologica, politica commerciale e continuità operativa dipendono da soggetti situati fuori dal proprio perimetro di controllo.

Dalla competizione tra prodotti alla competizione tra ecosistemi

Per questo la competizione nell'AI non può essere letta soltanto chiedendosi chi possieda il modello con il benchmark migliore.

Conta la capacità di calcolo, contano i modelli, contano i dati e le competenze. Ma contano anche distribuzione, utenti, cloud, integrazioni, developer, applicazioni e capacità finanziaria. In altre parole, la competizione si sposta sugli ecosistemi.

Più un ecosistema viene utilizzato, più diventa conveniente sviluppare applicazioni compatibili con esso; più applicazioni vengono sviluppate, più aumenta la sua utilità; più entra nei processi aziendali, maggiore può diventare il costo economico e organizzativo di sostituirlo.

Non serve quindi immaginare che ogni interazione venga utilizzata per addestrare il modello affinché si produca un effetto di concentrazione.

È sufficiente che utilizzo, distribuzione, integrazioni e investimenti si rafforzino reciprocamente.

Da questo punto di vista, il rischio per l'Europa non è semplicemente quello di “regalare i propri dati”. È più profondo: diventare un grande mercato di consumo e una grande fonte di conoscenza per infrastrutture cognitive delle quali controlla soltanto una parte limitata.

La risposta, però, non può essere l'autarchia tecnologica. La domanda strategica è capire quali dipendenze possiamo accettare senza perdere la capacità di scegliere, controllare e, quando necessario, cambiare.

Ed è precisamente qui che il problema della protezione del know-how aziendale incontra quello della sovranità tecnologica.

Perché se la conoscenza è una delle materie prime dell'economia dell'intelligenza artificiale, la domanda non è soltanto chi la produce. È anche chi controlla l'infrastruttura che la trasforma in valore.

Cosa significa “sovranità” nell’intelligenza artificiale

La parola sovranità è diventata una delle più utilizzate nel dibattito europeo sull'intelligenza artificiale e, proprio per questo, rischia di significare tutto e niente.

Sovranità tecnologica non significa necessariamente costruire un modello nazionale, possedere ogni data center, produrre ogni chip o rinunciare alle tecnologie sviluppate fuori dall'Europa. Un obiettivo del genere sarebbe, oltre che difficilmente realistico, contrario alla natura stessa di filiere tecnologiche globali e profondamente interdipendenti.

Sovranità significa non dipendere da qualcosa al punto da non poter più decidere.

Applicata all'intelligenza artificiale, questa capacità dipende da almeno cinque elementi.

La capacità di calcolo. Non è necessario che ogni impresa o ogni Stato possieda direttamente tutta l'infrastruttura di cui ha bisogno.

È però strategicamente rilevante poter accedere a capacità computazionale sufficiente attraverso infrastrutture e fornitori dei quali si conoscano giurisdizione, condizioni di servizio, dipendenze e possibilità alternative.

I dati. Significa sapere dove risiedono, chi può accedervi, quali informazioni possono essere utilizzate per quali finalità e quali garanzie esistono sul loro trattamento. Ma significa anche riconoscere che il valore non risiede soltanto nei database formalmente classificati: come abbiamo visto, può trovarsi nella combinazione di migliaia di frammenti apparentemente ordinari.



SOVRANITÀ NELL'INTELLIGENZA ARTIFICIALE

La capacità di scegliere, controllare e far evolvere le tecnologie critiche lungo tutta la catena del valore.

I modelli e gli algoritmi. Sovranità non significa necessariamente svilupparli tutti internamente. Significa poter scegliere tra alternative, comprendere sufficientemente i sistemi utilizzati, verificarne caratteristiche e vincoli e, dove necessario, poter ricorrere a modelli aperti o adattabili senza dipendere esclusivamente da sistemi sui quali non esiste alcuna possibilità di intervento.

Le competenze. Senza persone capaci di valutare, implementare, adattare e governare l'intelligenza artificiale, qualsiasi autonomia infrastrutturale rimane teorica. Un'organizzazione che possiede i dati e acquista il compute, ma non dispone delle competenze necessarie per comprendere ciò che sta utilizzando, continua a dipendere da chi quelle competenze le possiede.

La governance. È ciò che trasforma infrastrutture, dati, modelli e competenze in capacità di scelta. Comprende regole, responsabilità, procedure di controllo e criteri con cui stabilire quali sistemi possono essere utilizzati, per quali attività e con quali informazioni.

Nessuno di questi elementi, isolatamente, produce sovranità. Un data center europeo che ospita un sistema completamente incontrollabile non risolve il problema. Un modello europeo che dipende integralmente da infrastrutture esterne non lo risolve. Un modello open source senza competenze per gestirlo non lo risolve. E una normativa molto avanzata senza capacità tecnologica non basta.

La sovranità è nella combinazione

Ed è qui che il ragionamento torna al punto dal quale siamo partiti. La sovranità tecnologica europea può sembrare un tema distante dalla decisione di un dipendente che apre una finestra di chat e inserisce un documen-

to. In realtà i due livelli sono collegati: quella decisione stabilisce, in una misura infinitesimale ma concreta, dove passa la conoscenza, quale infrastruttura acquista centralità e quale dipendenza viene costruita.

Moltiplicata per milioni di persone, migliaia di imprese e centinaia di amministrazioni, la scelta individuale diventa una scelta di sistema.

Per questo la questione non è scegliere tra utilizzare o non utilizzare l'intelligenza artificiale. È costruire le condizioni per utilizzarla senza rinunciare alla capacità di scegliere dove far transitare la conoscenza, chi può elaborarla e quanto facilmente possiamo cambiare tecnologia quando le condizioni non sono più quelle che avevamo accettato.

Ed è proprio da qui che si passa dalla teoria alla pratica: che cosa può fare concretamente un'impresa?

Cosa si può fare davvero

Di fronte a un rischio che agisce contemporaneamente su due livelli, le contromisure più efficaci non sono soltanto di natura contrattuale, anche se avere policy e condizioni chiare resta essenziale, ma anche architetture, organizzativa e comportamentale. E producono un beneficio doppio: proteggono il patrimonio di conoscenza della singola azienda e, sommate su larga scala, contribuiscono a ridurre lo squilibrio competitivo più ampio.

Isolamento on-premise. Per le attività più sensibili, far funzionare i modelli su infrastrutture direttamente controllate dall'azienda può ridurre drasticamente l'esposizione della conoscenza verso l'esterno, a condizione che l'architettura sia realmente locale e correttamente configurata. L'on-premise non è automaticamente sinonimo di sicurezza: aumenta il controllo diretto sul trattamento delle informazioni, ma trasferisce sull'organizzazione anche la responsabilità di proteggere infrastruttura, modelli, accessi e dati.

Nessuna chiamata a servizi esterni. Un sistema apparentemente installato all'interno dell'azienda può continuare a utilizzare servizi esterni per elaborare parte del lavoro, effettuare aggiornamenti o accedere ad altre funzionalità. Per le attività che richiedono il massimo livello di isolamento è quindi necessario verificare l'intera architettura e assicurarsi che nessun frammento di informazione lasci il perimetro definito dall'organizzazione attraverso chiamate non previste o non controllate.

Air gapping dei sistemi più critici. Per categorie di informazioni particolarmente sensibili, come ad esempio ricerca e sviluppo,

formulazioni, processi produttivi distintivi, dati clinici o sperimentali, può essere opportuno mantenere ambienti fisicamente o logicamente separati dalle reti esterne, accessibili soltanto secondo procedure definite. È la soluzione più restrittiva e non può evidentemente diventare il modello per ogni utilizzo dell'AI, ma rimane uno strumento da considerare quando il valore della conoscenza giustifica il costo dell'isolamento.

Classificazione consapevole di ciò che può uscire e di ciò che deve restare all'interno.

Costruire e mantenere aggiornata una mappa condivisa delle attività che possono essere svolte attraverso strumenti esterni e di quelle che devono invece rimanere entro ambienti maggiormente controllati. La classificazione non dovrebbe riguardare soltanto i documenti già identificati come riservati, ma anche quei frammenti di conoscenza che, combinati con altri, possono contribuire all'effetto mosaico.

Formazione delle persone, non solo configurazione dei sistemi. Spiegare con esempi concreti, e non attraverso divieti generici, cosa può accadere a un'informazione una volta condivisa con un sistema esterno e quali differenze esistono tra gli strumenti autorizzati dall'azienda e quelli utilizzati attraverso account personali o servizi consumer. In questo caso, l'obiettivo non è tanto quello di impedire alle persone di utilizzare l'intelligenza artificiale, ma di renderle consapevoli del valore del contesto che forniscono per ottenere una risposta migliore.

Ambienti di sperimentazione separati.

Creare sandbox nelle quali le persone possano imparare a utilizzare gli strumenti e sperimentare nuovi casi d'uso senza esporre informazioni aziendali reali, ricorrendo quando possibile a dati sintetici, fittizi o opportunamente anonimizzati.

Controllo degli accessi e tracciabilità

interna. Sapere quali sistemi vengono utilizzati, da chi e per quali finalità, applicando controlli proporzionati alla sensibilità delle informazioni e alla criticità dei processi. La tracciabilità deve servire a ricostruire ciò che è accaduto in caso di dubbio o incidente e a verificare il rispetto delle regole aziendali, senza trasformarsi in una sorveglianza indiscriminata delle attività dei dipendenti.

Politiche contrattuali chiare quando si

utilizzano strumenti esterni. Verificare e, quando possibile, negoziare condizioni esplicite su conservazione dei dati, cancellazione, localizzazione, accesso da parte di terzi e utilizzo delle interazioni per training o miglioramento dei sistemi. Le condizioni applicate ai servizi enterprise possono essere molto diverse da quelle dei prodotti consumer: trattarle come se fossero equivalenti significa rinunciare a una parte importante della capacità di controllo.

Valutazione della giurisdizione e, quando appropriato, preferenza per infrastrutture e fornitori europei.

Non per un riflesso protezionistico e nemmeno perché un fornitore europeo sia automaticamente più sicuro. La localizzazione, la giurisdizione applicabile, l'architettura tecnica, le condizioni contrattuali e la possibilità di verificare i flussi informativi sono elementi distinti che devono essere valutati insieme. Quando un'infrastruttura europea offre condizioni tecnologiche adeguate e un maggiore controllo su questi elementi, utilizzarla può contribuire contem-

poraneamente alla protezione del know-how aziendale e allo sviluppo di un ecosistema tecnologico sul quale l'Europa conserva una maggiore capacità di influenza.

Nessuna di queste misure, presa da sola, è sufficiente.

La protezione reale nasce dalla combinazione di più livelli, tecnico, organizzativo, contrattuale e culturale, pensati insieme e non aggiunti uno alla volta dopo che un problema si è già manifestato.

La questione, in definitiva, non è scegliere tra utilizzare l'intelligenza artificiale e proteggere il proprio know-how. Un'impresa che rinunciasse ai migliori strumenti disponibili per paura di esporre la propria conoscenza rischierebbe di perdere competitività.

La sfida è quella di utilizzare l'AI decidendo consapevolmente quale conoscenza può uscire, attraverso quale infrastruttura e a quali condizioni. Perché, se l'effetto mosaico nasce dalla somma di migliaia di piccoli frammenti, anche la sovranità comincia dalla somma di migliaia di piccole decisioni.

Conclusioni. La sovranità comincia da un prompt

Il rischio più insidioso dell'intelligenza artificiale generativa per un'impresa non assume necessariamente la forma di un evento clamoroso. Può essere qualcosa di molto più lento e meno visibile: la progressiva trasformazione in informazione digitale di un patrimonio di conoscenza costruito in anni di esperienza, attraverso migliaia di interazioni che, considerate singolarmente, sembrano avere poco valore.

È l'effetto mosaico da cui siamo partiti. Nessuna tessera racconta da sola l'intera organizzazione. Ma ciò che conta non è soltanto il valore del singolo frammento: è ciò che può diventare conoscibile quando i frammenti vengono combinati, contestualizzati e messi in relazione.

La stessa dinamica, osservata da una distanza maggiore, pone una questione che riguarda l'intero sistema economico europeo.

L'Europa continua a produrre una straordinaria quantità di conoscenza industriale, scientifica, professionale e culturale, mentre una parte crescente delle infrastrutture attraverso cui quella conoscenza viene elaborata, organizzata e trasformata in servizi e valore economico è controllata da soggetti extraeuropei.

Questo non significa che ogni informazione affidata a un sistema di intelligenza artificiale venga automaticamente utilizzata per addestrarlo, né che utilizzare tecnologie sviluppate fuori dall'Europa equivalga a trasferire il proprio know-how a un concorrente. Il valore può essere catturato attraverso il training, ma anche attraverso distribuzione, integrazioni, casi d'uso, ecosistemi e dipendenze infrastruttu-

rali. La questione decisiva diventa allora chi produce la conoscenza e chi controlla l'infrastruttura capace di trasformarla in capacità tecnologica e valore economico.

Vista da vicino, è la scelta di un dipendente che apre una finestra di chat e decide quanto contesto fornire. Vista da lontano, è la scelta di un'impresa e, moltiplicata per migliaia di imprese, di un intero sistema industriale, su dove far transitare una delle proprie risorse più preziose.

Non si tratta di fermare questa circolazione, né di chiudere la conoscenza dentro un recinto ma di conservare la capacità di decidere.

Decidere quale conoscenza può uscire dall'organizzazione e quale deve restare al suo interno, attraverso quale infrastruttura può transitare, chi può elaborarla, per quali finalità e con quali garanzie.

È una questione che riguarda cloud, modelli, capacità di calcolo, contratti e governance. Ma può cominciare molto prima: da una persona davanti a un computer, da un problema da risolvere e da una domanda apparentemente innocua rivolta a un'intelligenza artificiale.

Perché quella domanda, da sola, può raccontare molto poco, ma può essere la prima tessera di un mosaico molto più grande.

Fonti e documenti

Kaplan, J. et al. (2020), Scaling Laws for Neural Language Models.
Hoffmann, J. et al. (2022), Training Compute-Optimal Large Language Models
OpenAI – Enterprise Privacy / Business Data.
OpenAI – How your data is used to improve model performance.
Anthropic – Is my data used for model training?
Microsoft – Data, privacy and security for Azure OpenAI.
Google Workspace – Generative AI privacy and security.
Commissione europea (2020), A European Strategy for Data, COM(2020) 66 final.
Commissione europea – European Data Strategy / Data Union Strategy.
Parlamento europeo e Consiglio dell'Unione europea (2016), Direttiva (UE) 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate.
Nonaka, I., Takeuchi, H. (1995), The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation, Oxford University Press.
Commissione europea (2025), AI Continent Action Plan.
Commissione europea, Strengthening Europe's Tech Sovereignty.
Commissione europea (2026), Proposal for the Cloud and AI Development Act (CADA), COM(2026) 502.
Commissione europea, Artificial Intelligence – Shaping Europe's Digital Future.
Bloomberg, Mark Gurman, Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak, 2 maggio 2023
Reuters, Apple restricts use of OpenAI's ChatGPT for employees, 18 maggio 2023
Reuters, Jeffrey Dastin e Anna Tong, Google, one of AI's biggest backers, warns own staff about chatbots, 15 giugno 2023
Bloomberg, William Shaw, JPMorgan Restricts Staff's Use of AI-Powered ChatGPT Bot, 22 febbraio 2023
Harmonic Security, GenAI Data Exposure Report, Q2 2025
Reuters, Dietrich Knauth, Google to buy Spirit Airlines business data for \$10 million, 17 agosto 2026
Wiz Research, ricerca sulla configurazione pubblicamente accessibile di un database DeepSeek, gennaio 2025

La selezione seguente raccoglie le principali fonti istituzionali, scientifiche e documentali utilizzate per la verifica delle informazioni e come riferimento per l'elaborazione delle analisi sviluppate nel Paper. Non costituisce una bibliografia esaustiva della letteratura sui temi trattati.

Nota metodologica

Il concetto di “effetto mosaico” viene utilizzato in questo Paper come chiave interpretativa per descrivere il valore informativo che può emergere dalla combinazione e contestualizzazione di frammenti di conoscenza aziendale singolarmente non necessariamente sensibili. Non viene proposto come categoria giuridica o tecnica formalmente codificata, ma come strumento di analisi del rapporto tra conoscenza tacita, utilizzo dell'intelligenza artificiale e sovranità tecnologica.

Disclaimer

Questa pubblicazione è stata realizzata da Rivista.AI con finalità di analisi, ricerca e posizionamento strategico e intende contribuire al dibattito sull'evoluzione dell'intelligenza artificiale e sui suoi effetti economici, industriali e tecnologici.

Le informazioni e le analisi contenute nel documento si basano su fonti pubbliche, dati istituzionali, letteratura scientifica, report di ricerca e documentazione disponibile alla data di chiusura editoriale. Pur essendo state sottoposte a verifica, tali informazioni possono essere soggette ad aggiornamenti, revisioni o differenti interpretazioni.

Il documento non costituisce parere legale o professionale. Le valutazioni e gli scenari presentati hanno finalità esclusivamente analitiche e non devono essere interpretati come previsioni certe di evoluzioni future.

Eventuali riferimenti ad aziende, piattaforme, prodotti o servizi sono utilizzati a fini esemplificativi e di analisi dell'evoluzione del mercato e non costituiscono endorsement, raccomandazioni né giudizi di merito sui singoli operatori.

Le interpretazioni e le conclusioni espresse nel Paper sono responsabilità editoriale di Rivista.AI.

Nota sull'utilizzo dell'intelligenza artificiale

Nella realizzazione di questo Paper sono stati utilizzati strumenti di intelligenza artificiale generativa come supporto ad alcune fasi del processo editoriale, in particolare per la realizzazione di elementi grafici come le immagini.

La scelta di dichiararne l'utilizzo risponde allo stesso principio di trasparenza e controllo delle tecnologie che costituisce uno dei temi centrali della serie di Paper di Rivista.AI sulla “Sovranità Tecnologica”.

L'impostazione del Paper, le tesi e i concetti interpretativi, la selezione e la valutazione delle evidenze e le conclusioni sono stati definiti, supervisionati e validati editorialmente da Rivista.AI.

Rivista.AI, elenco Paper Serie “Sovranità Tecnologica”

“Competitività digitale dell'Unione Europea: semiconduttori, infrastrutture cloud e AI nel contesto geopolitico 2026” - 06/2026

“La sovranità tecnologica nell'era dell'AI: la scommessa francese” - 07/2026

“La sovranità tecnologica europea nell'era dell'intelligenza artificiale. Proposta operativa” - 07/2026

“Dal modello alla fabbrica: perché la sovranità tecnologica è la sfida decisiva per l'industria italiana” - 07/2026

“La fabbrica invisibile: come l'intelligenza artificiale sta riscrivendo la visibilità dell'industria italiana nel mondo” - 09/2026