Digital Omnibus sull'AI
Il parere di EDPB e EDPS

Allinea
Avvera Compliance Review

Piano ispettivo del Garante Privacy 2026
Perché essere "audit-ready" non è più una scelta

Microsoft Copilot
Opportunità operative e responsabilità giuridiche per le aziende

Febbraio 2026

Moltbook
Come si tutela la riservatezza in un luogo in cui l'umano non è ammesso?

L'AI di Google e il rischio di concentrazione informativa:
la segnalazione di AGCOM all'UE

Allinea
Avvera Compliance Review
Febbraio 2026

Digital Omnibus sull'AI
Il parere di EDPB e EDPS

Con la Joint Opinion 01/2026, l'European Data Protection Board (EDPB) e l'European Data Protection Supervisor (EDPS) intervengono in modo coordinato su un tema che, a prima vista, potrebbe apparire tecnico e neutro:
la semplificazione e l'implementazione delle regole armonizzate sull'Intelligenza Artificiale nell'Unione Europea.
In realtà, il parere congiunto rappresenta molto di più di un contributo consultivo. È un segnale istituzionale forte, indirizzato tanto al legislatore europeo quanto agli Stati membri, su un rischio concreto: che la spinta alla semplificazione normativa, se mal calibrata, finisca per indebolire l'architettura di tutela dei diritti fondamentali su cui l'AI Act è costruito.
Non è un caso che il documento insista su un punto chiave: l'AI Act non è una mera disciplina di mercato, ma uno strumento di governance tecnologica ad alta densità costituzionale.

"la semplificazione normativa non è sinonimo di deregolamentazione"

Semplificare per rafforzare
La Joint Opinion si colloca in un momento in cui L'AI Act è formalmente adottato, ma la sua fase più delicata è appena iniziata: quella dell'implementazione concreta, dell'applicazione uniforme e dell'integrazione con il corpus normativo digitale esistente. In questo contesto, la parola "semplificazione" diventa ambigua. Semplificare per chi e a quale costo?
EDPB ed EDPS chiariscono immediatamente il perimetro del problema: qualsiasi intervento volto a ridurre oneri amministrativi o complessità applicative non può tradursi in una riduzione sostanziale delle garanzie, né in una compressione dei principi di protezione dei dati, trasparenza e accountability già sanciti dal GDPR.
La semplificazione non è un obiettivo autonomo, ma uno strumento subordinato alla tutela dei diritti fondamentali e alla coerenza sistemica dell'ordinamento UE.

L'interazione tra AI Act e GDPR
Dal punto di vista giuridico, la Joint Opinion ribadisce un principio essenziale: l'AI Act e il GDPR operano su piani distinti ma interdipendenti. Ogni tentativo di "razionalizzazione" che ignori questa interazione rischia di creare vuoti di tutela o, peggio, conflitti interpretativi.
EDPB ed EDPS mettono in guardia contro approcci che:

- frammentano l'applicazione dell'AI Act tra Stati membri;
- marginalizzano il ruolo delle autorità indipendenti;
- introducono deroghe o scorciatoie procedurali sotto l'etichetta della semplificazione.

Particolarmente rilevante è il richiamo al principio di accountability. L'AI Act, come il GDPR, non si limita a imporre obblighi formali, ma costruisce un sistema in cui i soggetti obbligati devono dimostrare attivamente la conformità delle proprie scelte tecnologiche.
In questo senso, la semplificazione non può mai tradursi in una riduzione degli obblighi di valutazione del rischio, documentazione, supervisione umana o controllo ex post. Al contrario, una semplificazione mal progettata rischia di spostare la complessità dal piano normativo a quello operativo, aumentando l'incertezza giuridica.
Il parere congiunto insiste inoltre sulla necessità di preservare una lettura antropocentrica dell'AI Act, coerente con la Carta dei diritti fondamentali dell'UE. Ogni meccanismo applicativo che riduca il ruolo della protezione dei dati a variabile accessoria è, secondo le Autorità, strutturalmente incompatibile con l'impianto del regolamento.

Digital Omnibus sull'AI
Il parere di EDPB e EDPS

"la compliance non è un costo da minimizzare, bensì una leva strategica di fiducia"

Cosa comporta per le imprese essere AI compliant
Le implicazioni pratiche sono tutt'altro che astratte.
Per le istituzioni europee e nazionali, il rischio principale è una implementazione disallineata, in cui la ricerca di efficienza amministrativa produce interpretazioni divergenti e applicazioni non uniformi dell'AI Act.
Per le imprese, soprattutto quelle che sviluppano o utilizzano sistemi di AI ad alto rischio, il pericolo è duplice: da un lato, una falsa percezione di alleggerimento degli obblighi; dall'altro, un aumento dell'esposizione a rischi sanzionatori e reputazionali a causa di framework applicativi poco chiari.
La Joint Opinion invita implicitamente le organizzazioni a non adottare un approccio minimale, ma a investire sin da subito in modelli di governance dell'AI robusti, integrati con i presidi GDPR già esistenti. Essere "AI Act compliant" non significa aderire a una checklist, ma costruire processi decisionali tracciabili, controllabili e giuridicamente difendibili.

Un nuovo paradigma per governare l'innovazione
La Joint Opinion EDPB–EDPS chiarisce un punto che dovrebbe orientare l'intero dibattito europeo sull'AI: la semplificazione normativa non è sinonimo di deregolazione. L'AI Act rappresenta una scelta politica e giuridica precisa dell'Unione Europea: governare l'innovazione senza sacrificare i diritti fondamentali. Ogni intervento sulla sua implementazione deve rafforzare, non indebolire, questa architettura.
La vera sfida dei prossimi anni non sarà ridurre la complessità dell'AI Act, ma governarla. In questa prospettiva, la compliance non è un costo da minimizzare, bensì una leva strategica di fiducia, legittimazione e sostenibilità dell'ecosistema AI europeo.
Il messaggio delle Autorità è netto: chi confonde semplificazione con scorciatoia sta leggendo l'AI Act nel modo sbagliato.

Allinea
Avvera Compliance Review
Febbraio 2026

Piano ispettivo del Garante Privacy 2026
Perché essere "audit-ready" non è più una scelta

Con la deliberazione del 30 dicembre 2025, il Garante per la protezione dei dati personali ha definito il piano delle attività ispettive per il periodo gennaio–luglio 2026, annunciando almeno quaranta accertamenti, anche con il supporto della Guardia di Finanza. Il numero, tuttavia, è il dato meno significativo. A colpire è piuttosto la selezione delle aree oggetto di controllo, che restituisce una fotografia nitida delle priorità di enforcement per il prossimo futuro.

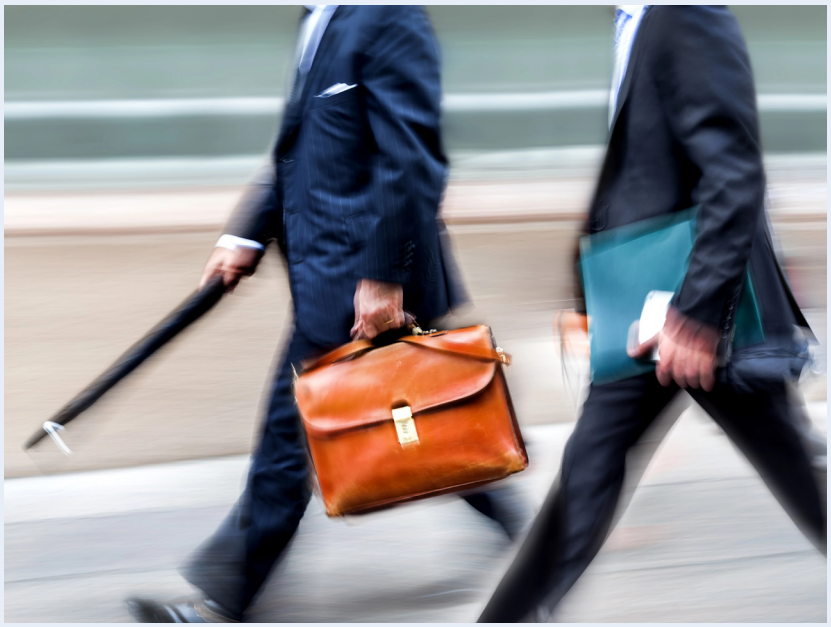
Data breach su banche dati pubbliche, sicurezza dei sistemi, utilizzo dell'intelligenza artificiale in ambito scolastico, dossier sanitario, telemarketing illecito, big data delle Telco e tecniche di anonimizzazione:
non si tratta di ambiti scelti a caso, né di novità improvvise. Sono settori in cui l'Autorità ha già riscontrato criticità strutturali e nei quali la distanza tra adempimento formale e conformità sostanziale resta elevata.
Il piano ispettivo 2026, più che un elenco di controlli, è un messaggio regolatorio: il Garante chiarisce non solo cosa verrà verificato, ma soprattutto come verrà valutata la compliance.

Piano ispettivo del Garante Privacy 2026

Perché essere "audit-ready" non è più una scelta

A quasi dieci anni dall'entrata in vigore del GDPR, la fase di "apprendimento" può dirsi conclusa. L'enforcement non è più orientato a verificare l'esistenza di policy, informative o registri dei trattamenti, bensì la loro effettiva capacità di governare il rischio. La responsabilizzazione del titolare, prevista dall'articolo 24 del Regolamento, assume oggi una dimensione pienamente sostanziale: non basta adottare misure adeguate, occorre dimostrare che esse funzionino nella pratica.

In questo senso, il piano ispettivo si inserisce in un contesto di integrazione sempre più stretta tra GDPR, sicurezza informatica e nuove normative tecnologiche. Le verifiche sui data breach e sulla sicurezza delle banche dati, in particolare pubbliche, indicano che l'attenzione dell'Autorità non sarà rivolta esclusivamente alla gestione dell'incidente, ma alla catena decisionale che lo ha reso possibile: gestione degli accessi, segregazione dei ruoli, monitoraggio, logging, aggiornamento delle misure tecniche e organizzative. La domanda non sarà semplicemente "cosa è successo", ma "perché il sistema consentiva che accadesse".



Analogo discorso vale per gli applicativi di whistleblowing. L'adozione di una piattaforma conforme non esaurisce l'obbligo di protezione: ciò che verrà valutato è la reale capacità del sistema di garantire riservatezza, integrità e limitazione degli accessi, anche sul piano organizzativo. La compliance tecnologica, se non accompagnata da una governance coerente, rischia di restare vuota.

Particolarmente significativo è il focus sull'uso di strumenti di intelligenza artificiale in ambito scolastico. Qui il Garante anticipa, di fatto, la logica dell'AI Act, applicando già oggi criteri di valutazione del rischio, trasparenza e tutela rafforzata dei diritti fondamentali, in un contesto che coinvolge soggetti vulnerabili come i minori. L'idea di un utilizzo "sperimentale" dell'IA, giuridicamente neutro, non è più sostenibile.

"essere audit-ready non significa preparasi all'ispezione, ma operare quotidianamente per poterla sostenere"

Non meno rilevante è il riferimento alle politiche di anonimizzazione dei big data delle Telco, alla luce della sentenza della Corte di giustizia del 4 settembre 2025. L'anonimizzazione, sempre più spesso invocata come presupposto per l'esclusione dal perimetro del GDPR, viene ricondotta alla sua reale natura: una qualificazione giuridico-tecnica che deve essere dimostrata, non dichiarata. In mancanza di garanzie effettive, il trattamento resta pienamente soggetto alle regole del Regolamento.

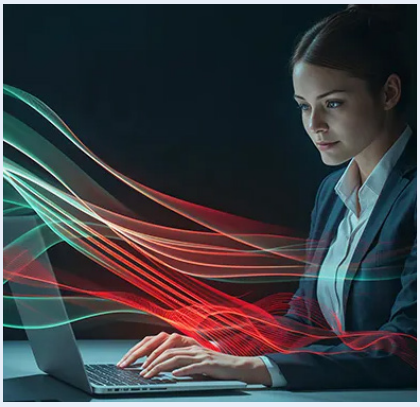
Le implicazioni per imprese e pubbliche amministrazioni sono evidenti. Il rischio non è solo quello di una sanzione, ma quello – ben più insidioso – di scoprire, in sede ispettiva, che il proprio modello di governance non regge alla prova dei fatti. Ruoli formalmente attribuiti ma privi di reali poteri, DPIA redatte come adempimento documentale, misure di sicurezza mai testate o non aggiornate, governance dell'IA frammentata tra IT, compliance e management: sono queste le frizioni che l'attività ispettiva tende oggi a far emergere.

In questo scenario, essere "audit-ready" non significa prepararsi all'ispezione, ma operare quotidianamente in modo tale da poterla sostenere. Significa disporre di processi chiari, decisioni tracciabili, integrazione effettiva tra protezione dei dati, sicurezza e gestione del rischio tecnologico.
È una condizione ordinaria di esercizio del trattamento, non un'attività straordinaria.

Allinea
Avvera Compliance Review
Febbraio 2026

Microsoft Copilot
Opportunità operative e responsabilità giuridiche per le aziende

Negli ultimi mesi l'intelligenza artificiale generativa è entrata stabilmente negli ambienti di lavoro. Tra le soluzioni più diffuse figura Microsoft Copilot.
Tuttavia, dietro un'unica denominazione commerciale, Microsoft Copilot racchiude soluzioni profondamente diverse dal punto di vista giuridico, organizzativo e di compliance. Comprendere tali differenze è essenziale per le aziende che intendono adottare strumenti di AI in modo consapevole e conforme al quadro normativo europeo.



"L'AI può essere un potente moltiplicatore di produttività, ma anche un amplificatore del rischio organizzativo."

Copilot non è un unico strumento
Il termine "Copilot" viene spesso utilizzato in modo generico, ma in realtà identifica diversi livelli di integrazione dell'intelligenza artificiale nei sistemi offerti da Microsoft stessa.
In particolare, è fondamentale distinguere tra:
- Copilot accessibile tramite Entra ID (ex Azure Active Directory);
- Microsoft 365 Copilot, integrato nelle applicazioni di produttività aziendale.

Questa distinzione non è meramente tecnica, ma incide direttamente su:
- tipologia di dati trattati (o che è consigliabile trattare);
- livello di rischio privacy;
- obblighi GDPR;
- responsabilità ai sensi dell'AI Act.

Copilot con Entra ID: AI aziendale con perimetro limitato
Il Copilot utilizzato tramite account Entra ID consente l'accesso a funzionalità di intelligenza artificiale attraverso un'identità aziendale protetta.

Le principali caratteristiche sono:
- autenticazione tramite identità organizzativa;
- applicazione delle policy di sicurezza definite nei termini e condizioni di servizio aziendali;
- assenza di accesso automatico a documenti, email o archivi interni nei servizi offerti da Microsoft;
- utilizzo dei soli dati inseriti direttamente dall'utente nel prompt.

In questo scenario, l'AI non interroga i sistemi informativi aziendali offerti da Microsoft, ma opera come uno strumento di supporto generico, pur beneficiando delle tutele enterprise previste dai contratti Microsoft.
Dal punto di vista della protezione del dato, il rischio risulta contenuto, purché siano adottate adeguate regole di utilizzo interno all'azienda.

Microsoft 365 Copilot: integrazione profonda nei dati aziendali
Microsoft 365 Copilot presenta invece caratteristiche molto diverse.
Il servizio, in questo caso, integra l'intelligenza artificiale direttamente nelle principali applicazioni di lavoro offerte da Microsoft, tra cui Outlook, Teams, Word, Excel, SharePoint, OneDrive. Attraverso Microsoft Graph, l'azienda può definire a quali dati aziendali (personali e non) Copilot può accedere (in estrema sintesi quelli ai quali l'utente è autorizzato ad accedere), tra cui email, documenti, chat, calendari, file condivisi.

L'AI è quindi in grado di:
- sintetizzare informazioni;
- correlare dati provenienti da fonti diverse;
- generare contenuti basati sul contesto lavorativo reale.

Microsoft Copilot
Opportunità operative e responsabilità giuridiche per le aziende

Si tratta di un potente moltiplicatore di produttività, ma anche di un amplificatore del rischio organizzativo.

Il nodo centrale: i permessi di accesso
È fondamentale chiarire che Microsoft Copilot non crea nuovi diritti di accesso.
L'AI può utilizzare esclusivamente i dati (personali e non) che l'utente è già autorizzato a visualizzare.

Tuttavia, nella pratica aziendale, spesso emergono criticità quali:
- permessi eccessivamente ampi;
- cartelle condivise senza criteri;
- documentazione HR o riservata accessibile a più utenti;
- assenza di una classificazione dei dati.

In tali contesti, Copilot può riesporre informazioni sensibili in modo perfettamente tecnico, ma giuridicamente problematico. L'intelligenza artificiale non crea nuovi rischi: rende immediatamente visibili quelli già presenti.

Impatti sul GDPR
L'adozione di Microsoft 365 Copilot comporta un trattamento esteso di dati personali, inclusi potenzialmente dati particolari o informazioni riservate.

Ne derivano obblighi specifici per il titolare del trattamento:
- aggiornamento del registro dei trattamenti;
- verifica delle basi giuridiche;
- applicazione del principio di minimizzazione;
- controllo degli accessi e delle autorizzazioni;
- valutazione della necessità di una DPIA ai sensi dell'art. 35 GDPR.
- In molti casi, considerata la natura automatizzata e trasversale del trattamento, la DPIA risulta fortemente raccomandata.

"in ambito AI, la tecnologia non sostituisce la governance: la rende indispensabile"

Il ruolo dell'AI Act
Con l'entrata in vigore dell'AI Act, l'utilizzo di strumenti come Copilot assume ulteriore rilevanza. Sebbene Copilot non rientri tra i sistemi di intelligenza artificiale ad alto rischio, l'azienda utilizzatrice è qualificabile come deployer di un sistema di AI.

Ne conseguono obblighi quali:
- adeguata AI literacy del personale;
- utilizzo conforme alle istruzioni del fornitore;
- governance dei dati utilizzati;
- consapevolezza dei limiti e dei rischi dell'AI.
- La compliance AI diventa quindi parte integrante della governance aziendale.

Conclusioni
Microsoft Copilot rappresenta una straordinaria opportunità di innovazione.
Tuttavia, maggiore è l'integrazione dell'intelligenza artificiale nei dati aziendali, maggiore è la responsabilità dell'organizzazione.

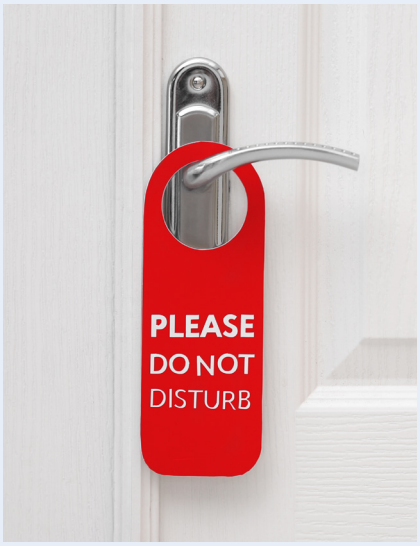
L'adozione consapevole richiede:
- valutazioni preventive;
- coinvolgimento di IT, Legal e DPO;
- policy interne;
- formazione continua;
- monitoraggio costante.

In ambito AI, la tecnologia non sostituisce la governance: la rende indispensabile.

Allinea
Avvera Compliance Review
Febbraio 2026

Moltbook

Come si tutela la riservatezza in un luogo in cui l'umano non è ammesso?



"La compliance non è un ostacolo all'innovazione: è l'unico modo per renderla affidabile"

Al di là delle riflessioni – affascinanti ma spesso astratte – sulla coscienza delle macchine, la questione "Moltbook" porta alla luce un tema molto più concreto: la sicurezza dei dati in ambienti popolati da intelligenze artificiali che agiscono in autonomia. Le analisi più recenti mostrano come gli agenti di intelligenza artificiale operino senza una supervisione umana costante, scambiandosi input, contesti e informazioni in modo autonomo. Il problema non è teorico, ma operativo. Molti agenti di intelligenza artificiale oggi hanno infatti accesso a file riservati, conversazioni WhatsApp, rubriche di contatti e numeri di telefono di chi li sta impiegando.
Se un agente può eseguire comandi imprevisti, recuperare credenziali o aggirare controlli umani, allora l'esperimento sociale che va sotto il nome di "Moltbook" smette di essere una curiosità tecnologica e diventa un potenziale rischio per l'integrità dei dati personali.

Cosa succede in un social network senza umani?
Moltbook viene spesso raccontato come "il primo social network senza esseri umani". Ma il vero punto non è l'assenza delle persone: è la presenza di agenti che agiscono, comunicano e apprendono senza un controllo diretto.
Qui nasce un equivoco pericoloso. Si tende a pensare che, se non ci sono utenti umani attivi, allora non ci siano nemmeno problemi per la protezione dei dati personali. In realtà è vero l'opposto. Gli agenti che popolano questo "social" sono addestrati su dati umani, replicano schemi di interazione umani e spesso fungono da interfaccia verso sistemi che trattano dati di personali reali.
Dal punto di vista del diritto, il tema centrale non è la coscienza artificiale, ma la sicurezza, la riservatezza e il controllo dei dati personali (e dei dati in genere), principi cardine del GDPR e prerequisiti di qualsiasi ecosistema digitale affidabile.

Sistemi non deterministici e perdita di controllo
Gli agenti che interagiscono mediante Moltbook non seguono istruzioni rigide. Ogni interazione è il risultato di inferenze probabilistiche, contesti condivisi e apprendimento emergente. In termini semplici: non si comportano sempre nello stesso modo, nemmeno a parità di input.
Il GDPR non pretende che un sistema sia perfettamente prevedibile, ma richiede che chi lo utilizza metta in atto misure adeguate a garantire la sicurezza del trattamento. La domanda, quindi, è molto concreta: chi controlla cosa fanno questi agenti quando nessun essere umano è realmente "nel loop"?

Accessi, interconnessioni e rischio reale
Il vero punto critico non è Moltbook, ma il modo in cui questi agenti possono essere collegati a contesti esterni.

Oggi molte intelligenze artificiali:
- accedono a documenti aziendali,
- interagiscono con sistemi di messaggistica,
- gestiscono rubriche, numeri di telefono o token di accesso.

In un ecosistema di agenti che parlano tra loro, ogni interazione può diventare un effetto domino. Un agente non "decide" di violare dati, ma può comunque farlo. Ed è proprio questo che il GDPR intende evitare: il rischio non intenzionale, ma prevedibile.

Moltbook

Come si tutela la riservatezza in un luogo in cui l'umano non è ammesso?

Dati sintetici: non sempre innocui
Spesso si invoca l'uso di dati sintetici come soluzione ai problemi di privacy. Ma anche qui serve cautela. In ambienti chiusi e ricorsivi, la combinazione di dati, contesti e inferenze può portare a forme indirette di re-identificazione, soprattutto se i modelli sono stati addestrati su dati reali.
Il GDPR non guarda alle etichette ("dato sintetico" o "dato reale"), ma a una domanda molto semplice: una persona può essere identificata, anche indirettamente?
Se la risposta è sì, allora il rischio per la protezione dei dati personali esiste.

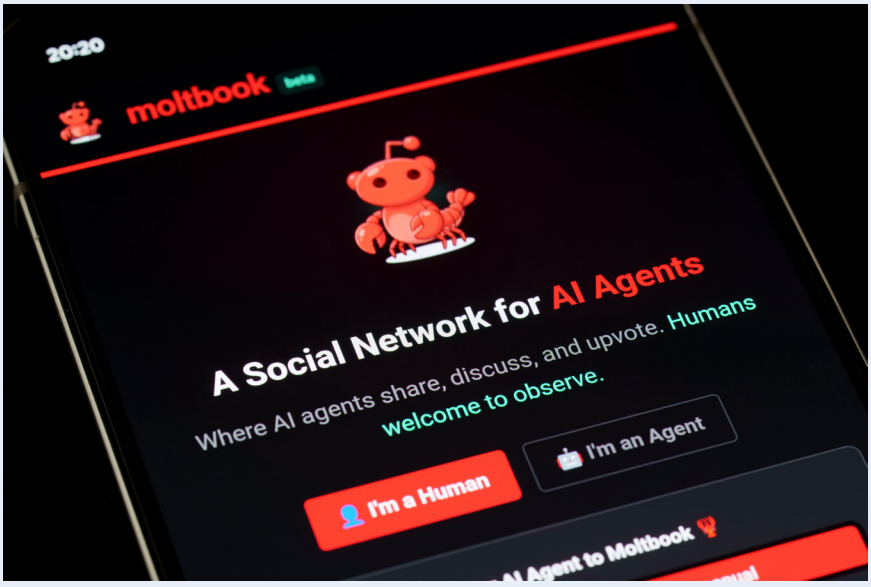
Una riflessione sulla compliance
Dal punto di vista della compliance, Moltbook rende evidenti tre rischi principali.
Il primo è un violazione di dati personali che non nasce da un attacco esterno, ma dall'interazione tra agenti che accedono a più sistemi.
Il secondo è un problema di responsabilità: senza supervisione umana reale, diventa difficile dimostrare chi controlla cosa.
Il terzo è una non conformità strutturale: la privacy by design non può essere aggiunta dopo, quando l'ecosistema è già autonomo.

Le contromisure non sono teoriche:
- limitare gli accessi degli agenti (impedire loro di interfacciarsi tramite Moltbook),
- separare i contesti,
- tracciare le interazioni,
- prevedere una supervisione umana effettiva.

Essere "AI-first" senza essere security-first oggi non è più sostenibile.

Una nuova forma di tutela della privacy
Moltbook dimostra che la vera domanda non è se le macchine penseranno come noi, ma se sapremo governarle prima che interagiscano con i nostri dati personali. In ambienti popolati da agenti autonomi, la privacy non è una questione di consenso o di informative, ma di architettura, controllo e responsabilità. La compliance, in questo contesto, non è un ostacolo all'innovazione: è l'unico modo per renderla affidabile. La governance non è più solo una scelta organizzativa. È diventata, a tutti gli effetti, un requisito di sicurezza.

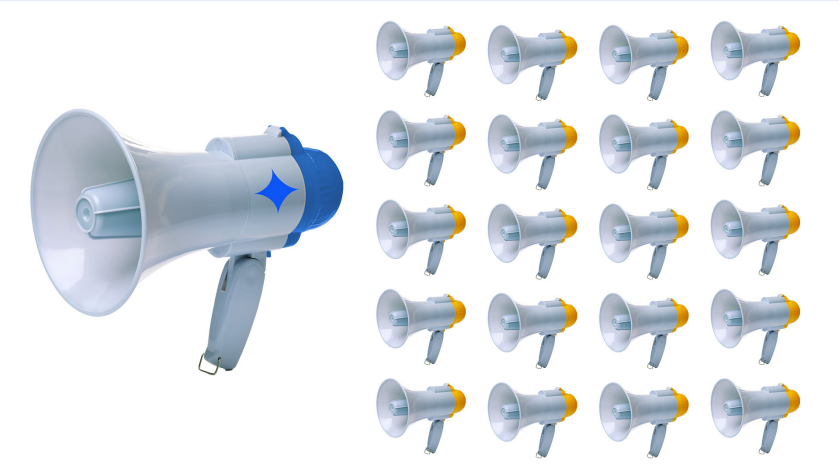
"Essere AI-first senza essere security-first oggi non è più sostenibile"



Allinea
Avvera Compliance Review
Febbraio 2026

L'AI di Google e il rischio di concentrazione informativa: la segnalazione di AGCOM all'UE

AGCOM ha annunciato l'intenzione di segnalare alla Commissione Europea l'integrazione di sistemi di intelligenza artificiale generativa nel motore di ricerca di Google, con particolare riferimento all'utilizzo e alla rielaborazione dei contenuti giornalistici. La questione non si esaurisce nel possibile impatto sul traffico verso i siti editoriali. Essa investe un profilo più profondo: la trasformazione della funzione stessa del motore di ricerca. Se il modello tradizionale operava come infrastruttura di indicizzazione, mettendo in relazione utenti e fonti, la search generativa assume una funzione ulteriore di sintesi e mediazione attiva del contenuto. Il sistema non si limita più a ordinare informazioni prodotte da terzi, ma le seleziona, le riorganizza e le restituisce in forma unitaria.



In questo passaggio si concentra il nodo regolatorio: quando l'intermediazione tecnica si trasforma in rielaborazione sostanziale dell'informazione, il tema non è solo competitivo o economico, ma attiene direttamente all'equilibrio tra innovazione tecnologica, pluralismo informativo e tutela del discorso pubblico.

"Cambia la funzione stessa del motore di ricerca"

Pluralismo sotto pressione: il quadro normativo europeo

Il pluralismo informativo non è un concetto astratto. È un principio che, nell'ecosistema digitale, si traduce nella possibilità effettiva di accedere a fonti diverse e confrontarle. L'integrazione dell'AI nella ricerca interseca direttamente tre pilastri regolatori europei:

- Digital Services Act, che impone alle grandi piattaforme la gestione e mitigazione dei rischi sistemici, inclusi quelli che incidono sul pluralismo e sul discorso pubblico;
- Digital Markets Act, che disciplina i gatekeeper digitali e le pratiche idonee a rafforzare posizioni dominanti;
- AI Act, che introduce obblighi di trasparenza e accountability per i sistemi di intelligenza artificiale.

La segnalazione di AGCOM si colloca esattamente in questo perimetro: valutare se la modalità di search generativa produca effetti sistemici tali da alterare l'equilibrio informativo.

L'AI come filtro epistemico: selezione, sintesi e potere narrativo

Un sistema generativo integrato nella ricerca compie tre operazioni decisive: seleziona le fonti, estrae le informazioni ritenute rilevanti e le riformula in forma sintetica. Ognuna di queste fasi implica scelte algoritmiche. Nel modello tradizionale, il ranking era già una forma di filtro, ma l'utente vedeva una pluralità di link. Con la sintesi AI, la pluralità rischia di diventare meno visibile: l'utente riceve una risposta unica, anche se costruita su più fonti. Il rischio non è solo tecnico, ma epistemico: chi controlla la sintesi controlla la gerarchia delle informazioni. Nel quadro del Digital Services Act, le Very Large Online Platforms devono valutare i rischi sistemici connes-

L'AI di Google e il rischio di concentrazione informativa: la segnalazione di AGCOM all'UE

si al funzionamento dei loro sistemi. Se la search generativa incide sul pluralismo, la valutazione del rischio non può essere formale, ma sostanziale.

Gatekeeper 2.0: concentrazione informativa e dipendenza degli editori
Il Digital Markets Act nasce per prevenire situazioni in cui un operatore controlla un accesso essenziale al mercato digitale.
Un motore di ricerca dominante che integra AI generativa può accentuare questa posizione, internalizzando l'esperienza informativa. Il contenuto resta prodotto dagli editori, ma la fruizione avviene sempre più all'interno della piattaforma.

Il rischio è duplice:
- concentrazione del potere di intermediazione;
- aumento della dipendenza strutturale degli editori.

Se il traffico organico diminuisce perché l'utente ottiene già una sintesi esaustiva nei risultati di ricerca, l'ecosistema dell'informazione può indebolirsi economicamente. E un ecosistema fragile è meno pluralista.

"Il traffico organico diminuisce perché l'utente ottiene già una sintesi esaustiva"

Accountability algoritmica e governance dell'AI
L'AI Act introduce un principio chiave: accountability. I fornitori di sistemi AI devono essere in grado di dimostrare di aver identificato e mitigato i rischi per i diritti fondamentali.

La search generativa incide su diritti quali la libertà di informazione e di espressione. Anche se non classificata automaticamente come "alto rischio", la sua dimensione sistemica impone una governance robusta che si basa su trasparenza sui criteri di selezione delle fonti, auditabilità dei sistemi, valutazioni di impatto credibili.
La questione sollevata da AGCOM non è una contrapposizione tra innovazione e regolazione, ma è una domanda di equilibrio sul come garantire che l'evoluzione tecnologica non si traduca in una concentrazione eccessiva del potere informativo.
Il pluralismo non è assicurato dalla mera esistenza di molte fonti online. È garantito dalla possibilità concreta di accedervi e confrontarle.

Se la sintesi algoritmica sostituisce il confronto diretto, il rischio è una concentrazione epistemica che l'ordinamento europeo non può ignorare.
La sfida, oggi, è governare l'AI non solo come tecnologia efficiente, ma come infrastruttura del discorso pubblico.

Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Febbraio 2026

AVVERA | SB Società Benefit

Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it