Intelligenza Artificiale e Privacy: i nostri dati sono davvero al sicuro?

Maria Cattini | 29/05/2025 | Intelligenza Artificiale

□□ Hai mai pensato a dove finiscono i tuoi dati?

Dai prompt inseriti su ChatGPT alle immagini caricate su Midjourney, passando per le ricerche su Gemini o Copilot: ogni interazione con un sistema basato sull'**Intelligenza Artificiale** lascia tracce. Ma chi controlla queste informazioni? E soprattutto, **quanto sono protette**?

Con la crescita esplosiva dell'**AI generativa**, la privacy personale è diventata una vera emergenza. E mentre si moltiplicano le segnalazioni di furti di dati e fughe di informazioni, l'Unione Europea prova a correre ai ripari. Vediamo cosa s□e davvero ai nostri dati.

⚠ I rischi della privacy nell'era dell'intelligenza artificiale

□□ Raccolta dati senza controllo

Gli algoritmi si nutrono di **quantità immense di dati**, spesso raccolti senza autorizzazione esplicita. Nomi, immagini, messaggi vocali, indirizzi IP. Molti utenti condividono informazioni sensibili senza saperlo, perché nessuno li ha davvero informati.

□□ Profilazione nascosta

Anche se non riveliamo esplicitamente le nostre preferenze, l'AI può **dedurre abitudini, orientamento politico o salute mentale** da comportamenti apparentemente innocui. Il risultato? Profili dettagliati, usati per influenzarci o venderci qualcosa.

□□ Incidenti e vulnerabilità

Il 97% delle aziende che usano AI generativa ha registrato almeno **un episodio di violazione dei dati**. Molte di queste falle nascono da errori umani o mancati controlli interni. A volte è sufficiente un prompt sbagliato per far trapelare informazioni riservate.

□□ AI e sorveglianza: fino a dove può spingersi?

Nei luoghi di lavoro o nelle città, l'AI viene spesso impiegata per **monitorare comportamenti, spostamenti, espressioni facciali**. Il confine tra sicurezza e intrusione si fa sottile. E in alcuni casi, invisibile.

□□ GDPR + AI Act: le nuove regole europee

□□□□ Il ruolo del GDPR

Il Regolamento Generale sulla Protezione dei Dati obbliga chi tratta dati personali a garantire:

© 2026 Coondivido — Tutti i diritti sono riservati

• chiarezza nelle finalità
• limitazione dell’uso
• sicurezza nell’archiviazione
• diritti esercitabili dall’interessato

Nel contesto AI, ogni trattamento va **valutato in anticipo** con una DPIA (valutazione d’impatto).

□□ AI Act: cosa cambia

Approvato nel 2024, entrerà in vigore pienamente nel 2026. Il regolamento **classifica i sistemi AI per rischio** e introduce obblighi precisi per quelli “ad alto rischio”. Tra i requisiti:

• supervisione umana obbligatoria
• documentazione tecnica dettagliata
• tracciabilità dei dati usati

□□□□ E in Italia?

Il Garante Privacy ha sanzionato OpenAI per violazioni nell’uso di ChatGPT, imponendo **misure correttive e campagne informative**. Un precedente importante per l’intero settore.

□□ Come proteggere davvero i dati personali?

□□ Privacy by design (e by default)

Chi sviluppa sistemi AI deve integrare **la tutela della privacy fin dall’inizio**. Non è un’aggiunta, ma una parte del progetto.

□□ Dati sintetici e anonimizzazione

Allenare modelli AI con dati “falsi” ma statisticamente realistici riduce il rischio di re-identificazione. Tecniche come la **differential privacy** aumentano la sicurezza.

□□ Informare in modo chiaro

Molti utenti non sanno cosa accade ai propri dati. **Le informative devono essere semplici**, leggibili, trasparenti. Non 18 pagine in legalese.

□□ Controllo umano

Secondo l’AI Act, **nessuna decisione automatica ad alto impatto può essere presa senza un supervisore umano**. È un punto chiave per evitare abusi.

□□ Innovazioni etiche

Tra le soluzioni emergenti:

• apprendimento federato (l’AI apprende senza accedere direttamente ai dati)
• crittografia avanzata
• firewall intelligenti per dati sensibili

□Siamo davvero protetti?

In teoria, **l’Europa ha il sistema normativo più solido al mondo**. In pratica, la corsa tecnologica è più veloce delle leggi. E mentre aziende e legislatori provano a recuperare terreno, resta a noi

© 2026 Coondivido — Tutti i diritti sono riservati

utenti il compito di essere più consapevoli.

□□ Checklist per la tua sicurezza digitale

□ Non inserire dati personali nei prompt AI
□ Usa AI solo su piattaforme trasparenti e verificate
□ Leggi (davvero) le informative privacy
□ Attiva la verifica a due fattori sui tuoi account
□ Tieni aggiornati antivirus e browser
□ Evita di usare AI per comunicazioni lavorative riservate

□□ Il futuro? Serve vigilanza (umana)

L'intelligenza artificiale continuerà a evolversi. Ma anche il concetto di privacy deve farlo. Servono leggi chiare, controlli reali e maggiore **alfabetizzazione digitale**. Solo così potremo davvero convivere con l'AI senza rinunciare alla nostra libertà.

□□ Vuoi saperne di più?

Iscriviti alla newsletter **"OSINT & AI per tutti"** per ricevere aggiornamenti pratici, casi reali e strumenti per proteggere i tuoi dati nel mondo digitale.
□□ Hai mai pensato a dove finiscono i tuoi dati?

Dai prompt inseriti su ChatGPT alle immagini caricate su Midjourney, passando per le ricerche su Gemini o Copilot: ogni interazione con un sistema basato sull'**Intelligenza Artificiale** lascia tracce. Ma chi controlla queste informazioni? E soprattutto, **quanto sono protette**?

Con la crescita esplosiva dell'**AI generativa**, la privacy personale è diventata una vera emergenza. E mentre si moltiplicano le segnalazioni di furti di dati e fughe di informazioni, l'Unione Europea prova a correre ai ripari. Vediamo cosa s□e davvero ai nostri dati.

⚠ I rischi della privacy nell'era dell'intelligenza artificiale

□□ Raccolta dati senza controllo

Gli algoritmi si nutrono di **quantità immense di dati**, spesso raccolti senza autorizzazione esplicita. Nomi, immagini, messaggi vocali, indirizzi IP. Molti utenti condividono informazioni sensibili senza saperlo, perché nessuno li ha davvero informati.

□□ Profilazione nascosta

Anche se non riveliamo esplicitamente le nostre preferenze, l'AI può **dedurre abitudini, orientamento politico o salute mentale** da comportamenti apparentemente innocui. Il risultato? Profili dettagliati, usati per influenzarci o venderci qualcosa.

□□ Incidenti e vulnerabilità

Il 97% delle aziende che usano AI generativa ha registrato almeno **un episodio di violazione dei dati**. Molte di queste falle nascono da errori umani o mancati controlli interni. A volte è sufficiente un prompt sbagliato per far trapelare informazioni riservate.

□□ AI e sorveglianza: fino a dove può spingersi?

Nei luoghi di lavoro o nelle città, l'AI viene spesso impiegata per **monitorare comportamenti, spostamenti, espressioni facciali**. Il confine tra sicurezza e intrusione si fa sottile. E in alcuni casi, invisibile.

© 2026 Coondivido — Tutti i diritti sono riservati

□□ GDPR + AI Act: le nuove regole europee

□□□□ Il ruolo del GDPR

Il Regolamento Generale sulla Protezione dei Dati obbliga chi tratta dati personali a garantire:

• chiarezza nelle finalità
• limitazione dell'uso
• sicurezza nell'archiviazione
• diritti esercitabili dall'interessato

Nel contesto AI, ogni trattamento va **valutato in anticipo** con una DPIA (valutazione d'impatto).

□□ AI Act: cosa cambia

Approvato nel 2024, entrerà in vigore pienamente nel 2026. Il regolamento **classifica i sistemi AI per rischio** e introduce obblighi precisi per quelli "ad alto rischio". Tra i requisiti:

• supervisione umana obbligatoria
• documentazione tecnica dettagliata
• tracciabilità dei dati usati

□□□□ E in Italia?

Il Garante Privacy ha sanzionato OpenAI per violazioni nell'uso di ChatGPT, imponendo **misure correttive e campagne informative**. Un precedente importante per l'intero settore.

□□ Come proteggere davvero i dati personali?

□□ Privacy by design (e by default)

Chi sviluppa sistemi AI deve integrare **la tutela della privacy fin dall'inizio**. Non è un'aggiunta, ma una parte del progetto.

□□ Dati sintetici e anonimizzazione

Allenare modelli AI con dati "falsi" ma statisticamente realistici riduce il rischio di re-identificazione. Tecniche come la **differential privacy** aumentano la sicurezza.

□□ Informare in modo chiaro

Molti utenti non sanno cosa accade ai propri dati. **Le informative devono essere semplici**, leggibili, trasparenti. Non 18 pagine in legalese.

□□ Controllo umano

Secondo l'AI Act, **nessuna decisione automatica ad alto impatto può essere presa senza un supervisore umano**. È un punto chiave per evitare abusi.

□□ Innovazioni etiche

Tra le soluzioni emergenti:

• apprendimento federato (l'AI apprende senza accedere direttamente ai dati)
• crittografia avanzata
• firewall intelligenti per dati sensibili

© 2026 Coondivido — Tutti i diritti sono riservati

Siamo davvero protetti?

In teoria, **l’Europa ha il sistema normativo più solido al mondo**. In pratica, la corsa tecnologica è più veloce delle leggi. E mentre aziende e legislatori provano a recuperare terreno, resta a noi utenti il compito di essere più consapevoli.

Checklist per la tua sicurezza digitale

 Non inserire dati personali nei prompt AI
 Usa AI solo su piattaforme trasparenti e verificate
 Leggi (davvero) le informative privacy
 Attiva la verifica a due fattori sui tuoi account
 Tieni aggiornati antivirus e browser
 Evita di usare AI per comunicazioni lavorative riservate

Il futuro? Serve vigilanza (umana)

L’intelligenza artificiale continuerà a evolversi. Ma anche il concetto di privacy deve farlo. Servono leggi chiare, controlli reali e maggiore **alfabetizzazione digitale**. Solo così potremo davvero convivere con l’AI senza rinunciare alla nostra libertà.

Vuoi saperne di più?

Iscriviti alla newsletter **“OSINT & AI per tutti”** per ricevere aggiornamenti pratici, casi reali e strumenti per proteggere i tuoi dati nel mondo digitale.

© 2026 Coondivido — Tutti i diritti sono riservati