

NOTIZIARIO **PRIVACY**

2026



→ **IA & PRIVACY**
Aziende
Cambiamenti
Responsabilità

NOTIZIARIO PRIVACY EURISTICA
Aprile-Maggio 2026

Fonti articoli

Federprivacy | federprivacy.org

Il Sole24Ore | www.ilsole24ore.com

Layout

Euristica

Crediti fotografici

Freepik, Canva, Federprivacy

Euristica è iscritta a Federprivacy dal 2018

4

IA in Azienda

L'82% investe ma mancano gli esperti!

8

IA in Azienda

Il cambiamento che le aziende stanno sottostimando

12

Privacy del cliente

il nuovo asset strategico

14

IA in Azienda

Non è solo di tecnologia ma la sfida di governare

16

GDPR

L'Accountability non è un'emergenza
ma un processo strategico

IA in Azienda

L'82% investe ma mancano gli esperti!

Fonte: Freepik



Mentre l'Europa definisce i contorni normativi con l'AI Act, l'Italia vive un momento di profonda contraddizione: un'accelerazione tecnologica senza precedenti che non trova riscontro nella preparazione dei suoi professionisti di punta.

La Corsa agli Investimenti: L'82% è già in campo

Il dato fornito da **Federprivacy** parla chiaro: l'Intelligenza Artificiale non è più una sperimentazione per pochi, ma una priorità per la stragrande maggioranza delle imprese **(82%)**

- **Obiettivo:** Ottimizzazione dei processi, riduzione dei costi e analisi predittiva.
- **Settori chiave:** Dalla manifattura avanzata al settore bancario, fino alla pubblica amministrazione.

Il Gap delle Competenze: I numeri della crisi

Nonostante i capitali siano pronti, le aziende si scontrano con un muro: la mancanza di figure tecniche e giuridiche specializzate.

- Non mancano solo i programmatori (AI Engineer), ma mancano soprattutto i "regolatori interni".
- Senza esperti in grado di comprendere l'algoritmo, l'azienda opera in un regime di "scatola nera" (black box), dove le decisioni automatizzate sfuggono al controllo umano.

L'82% delle aziende investe, ma meno del 20% dichiara di avere internamente le competenze necessarie per gestire la transizione in sicurezza.

La Diagnosi di Federprivacy: L'inerzia dei DPO

Il punto più critico evidenziato dall'associazione riguarda i Data Protection Officer (DPO) e i consulenti della privacy.

- **L'Opportunità:** Il DPO è, per natura, il professionista più vicino alla gestione dei rischi informativi. L'IA è alimentata da dati; pertanto, chi governa i dati dovrebbe governare l'IA.
- **La Criticità:** Molti professionisti percepiscono l'IA come un ambito puramente informatico o troppo complesso, rinunciando a formarsi.

Questo crea un **vuoto di governance**: le aziende comprano software di IA, ma nessuno ne verifica la conformità etica e legale (Privacy by Design).

Conseguenze e Rischi Operativi

L'assenza di esperti porta a tre rischi principali:

1. Sanzioni Regolatorie: Violazioni dell'IA Act e del GDPR.
2. Bias e Discriminazione: Algoritmi che operano scelte discriminatorie nel recruiting o nel credito.
3. Perdita di Proprietà Intellettuale: Dati aziendali sensibili "pasturati" a modelli di IA generativa pubblici senza filtri.



Fonte : ilsole24ore

Le 3 Competenze richieste

1. **AI Impact Assessment:** Valutare l'impatto dei sistemi algoritmici sui diritti fondamentali.
2. **Data Quality Management:** Verificare che i dati usati per l'addestramento non siano viziati.
3. **Governance Etica:** Definire linee guida interne per l'uso dell'IA generativa tra i dipendenti.

Le 5 cose da fare prima dell'audit

Aggiornare la documentazione con quella inviata dopo l'ultimo audit

Non significa necessariamente stampare tutto ciò che viene inviato volta per volta: come ricordiamo sempre a tutti, l'unico documento che va obbligatoriamente stampato e tenuto in ogni sua copia è il registro dei trattamenti, tutti gli altri file possono essere tranquillamente tenuti all'interno di una cartella digitale, anche le scansioni dei

Avere i documenti pronti a portata di mano (e di mouse) riduce significativamente tempi di intervento e ci permette di lavorare al meglio. i.

Preparare il faldone con tutta la documentazione, che sia in formato cartaceo o digitale

Controllare di aver seguito i consigli dati nell'ultima e-mail di aggiornamento documenti ricevuta (o nell'ultimo audit)

Seguire i nostri consigli è quello che rende possibile una gestione corretta e precisa di tutta la privacy aziendale.

Per redigere in maniera esaustiva e complessiva alcuni documenti serve l'accesso ai vari asset aziendali, quindi tutti i dispositivi aziendali utilizzati dovrebbero trovarsi in sede nel momento dell'audit e, allo stesso modo, tutti i dispositivi dovrebbero essere accessibili per un controllo e non bloccati da password.

Rendere possibile l'accesso a tutti gli asset aziendali che saranno sottoposti a controllo privacy

Informare tutte le persone coinvolte

Informare sempre il personale interessato (responsabili IT, amministrazione, responsabili privacy) dell'attività che si sta per svolgere e di conseguenza su orari e modalità del controllo.

IA in Azienda

Il cambiamento che le aziende stanno sottostimando

L'IA sta rivoluzionando il lavoro, creando nuove professioni e richiedendo competenze innovative, con i giovani che fanno protagonisti nell'adozione e nell'uso strategico di queste tecnologie

L'intelligenza artificiale non è più una scommessa per il futuro, ma una realtà che sta riscrivendo le regole della leadership e della strategia aziendale. Tuttavia, nonostante l'accelerazione tecnologica, molte imprese italiane rischiano di restare indietro a causa di una visione ancora troppo limitata e specialistica.

Diffusione Esponenziale: Entro il 2026, si stima che il 90% delle aziende avrà integrato l'IA nei propri piani strategici, elevandola a una delle prime tre priorità di business. Attualmente, però, solo un'azienda su quattro ha un piano strutturato.

Fonte: Freepik



Il Problema della "Shadow AI":

Emerge il fenomeno dell'IA "sommersa": i dipendenti utilizzano strumenti di intelligenza artificiale in modo autonomo e individuale per migliorare la propria produttività, ma spesso senza una guida o una condivisione con il manager, creando un divario di competenze interno.

Oltre le Stanze dei Tecnici: Il vero potenziale dell'IA si sprigiona solo quando esce dai dipartimenti IT per diventare patrimonio comune. Ad oggi, la formazione è il grande collo di bottiglia: solo il 6% dei lavoratori possiede competenze adeguate.

Fonte: Canva



L'IA non segna la fine del lavoro, è l'inizio di un lavoro migliore

Sempre più spesso sono i giovani a insegnare ai colleghi senior come utilizzare gli strumenti che stanno ridefinendo il lavoro moderno, lo dimostra anche una recente ricerca che abbiamo realizzato come International Workplace Group (IWG) in cui si evidenzia come i dipendenti della Generazione Z siano diventati protagonisti nell'adozione dell'AI, promotori del suo utilizzo in azienda.

Umanesimo Industriale: La sfida del futuro non sarà la sostituzione dell'uomo, ma il divario tra chi saprà collaborare con l'IA e chi no. La leadership deve evolvere per gestire questo cambiamento culturale, garantendo che la tecnologia supporti il lavoro umano invece di alienarlo.

Fonte: IlSole24Ore

Dieci Regole e Suggerimenti per un utilizzo corretto e funzionale dell'IA

1. DATI AZIENDALI

Non inserire ragioni sociali, documenti aziendali riservati, analisi specifiche, riferimenti a progetti interni, database e loro parti, documenti di testo ed Excel, in sintesi tutto ciò che è legato all'ambito lavorativo, a colleghi, clienti e fornitori
Inserire dati in un motore AI equivale a perderli e le perdite di dati aziendali sono penalmente perseguibili.

2. DATI PERSONALI

Non inserire i tuoi dati personali né quelli altrui, non inserire nomi e cognomi, numeri di telefono, indirizzi fisici o digitali, foto, video né documenti medici
Il GDPR ci protegge se noi siamo in grado di farci proteggere, se spargiamo dati come fossero semi non faranno che crescere problemi

3. PROMPTING

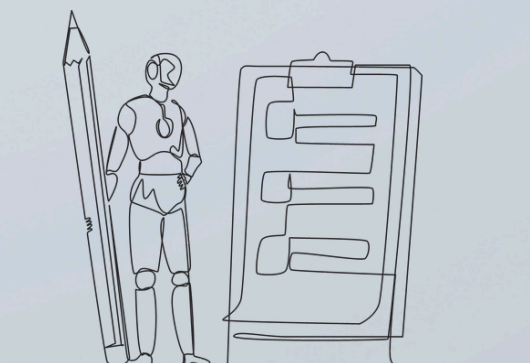
Scrivi richieste chiare e generiche, evitando riferimenti a dati sensibili o contesti riservati, rileggi prima di inviare e assicurati di non aver inserito dati e di aver posto la domanda corretta
Un prompt mal formulato può causare la diffusione involontaria di informazioni critiche.

4. FONTI

Controlla sempre l'attendibilità delle risposte dell'IA, confrontandole con fonti ufficiali (fai particolare attenzione ai motori di ricerca integrati con le IA).
Un prompt mal formulato può causare la diffusione involontaria di informazioni critiche.

5. LIMITI

Ricorda che l'IA non ha coscienza, non comprende il contesto umano e non deve (per legge) mai sostituire la coscienza umana nel processo di presa di decisioni
Usarla come unico strumento decisionale può generare rischi operativi, legali ed etici.



Dieci Regole e Suggerimenti per un utilizzo corretto e funzionale dell'IA

6. ATROFIA TECNOLOGICA

Usare l'AI come strumento, non come sostituto totale del pensiero critico o del lavoro e delle capacità umane
La dipendenza dall'IA può ridurre competenze, autonomia, abilità e capacità di giudizio

7. FORMAZIONE

Aggiornati costantemente su strumenti, rischi, buone pratiche e novità legate al mondo dell'IA
Il mondo dell'IA è in costante e veloce sviluppo, fare del proprio meglio per restare aggiornati è fondamentale

8. ETICA E RESPONSABILITÀ

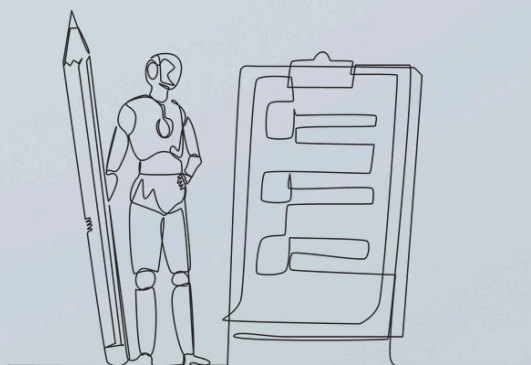
Usa l'IA in modo equo, rispettoso e trasparente, evitando discriminazioni e manipolazioni
Un uso scorretto può danneggiare persone, aziende e società, anche legalmente

9. CONTESTO D'USO

Valuta sempre dove, come e perché stai usando l'IA. ogni ambiente ha regole e sensibilità diverse
Un uso fuori contesto può causare fraintendimenti, violazioni e danni reputazionali

10. SEGNALAZIONE

Segnala qualsiasi uso improprio dell'intelligenza artificiale
Far notare che si sta utilizzando l'IA in modo sbagliato è innocuo e salvaguarda potenziali problematiche di rilievo



Privacy del cliente

Il nuovo asset strategico

"In un mercato saturo di prodotti simili, la differenza non la fa più solo il prezzo, ma la fiducia. Oggi la privacy non è più un mero adempimento burocratico da confinare negli uffici legali, ma il vero motore della competitività: chi protegge i dati, conquista il cliente."

Dal "Compliance" al "Competitive Advantage"

Il report di Federprivacy evidenzia un cambio di paradigma radicale. Le aziende che superano la visione della protezione dati come "costo necessario" stanno scoprendo che la trasparenza attira investitori e

consumatori sempre più consapevoli. La privacy diventa quindi un marchio di qualità che distingue il brand in un ecosistema digitale spesso percepito come insicuro.

La Tutela dei Dati per la Customer Retention

I dati parlano chiaro: la perdita di dati (data breach) non causa solo sanzioni pecuniarie, ma un danno reputazionale spesso irreversibile. Al contrario, una gestione etica dei dati personali aumenta la fidelizzazione del cliente, riducendo il tasso di abbandono e trasformando l'utente in un alleato del brand.

L'Impatto sull'Innovazione e l'Intelligenza Artificiale

Con l'avvento dell'IA, la qualità e l'eticità del dato sono diventate cruciali. Federprivacy sottolinea come le aziende "Privacy-First" siano più pronte a implementare tecnologie avanzate senza incorrere in blocchi normativi o crisi di fiducia, garantendo una scalabilità del business più fluida e sicura.

Fonte: Federprivacy



Fonte: Federprivacy



Il Ruolo del DPO e del Management

La competitività passa attraverso una governance solida. Il sommario mette in luce la necessità di un dialogo costante tra il Data Protection Officer e il board aziendale: la privacy deve essere integrata fin dalla progettazione (Privacy by Design) di ogni nuovo prodotto o servizio per massimizzare il ritorno sull'investimento.

La protezione dei dati è passata dall'essere un freno a mano a un acceleratore di business. Le aziende che sapranno comunicare il proprio valore etico nella gestione delle informazioni saranno le leader del mercato di domani.

IA IN AZIENDA

Non è solo tecnologia ma la sfida di governance

L'intelligenza artificiale non è più un semplice esperimento tecnico nei dipartimenti IT, ma un vero e proprio processo aziendale che richiede una guida strategica. Secondo un recente approfondimento di Federprivacy, il successo (e la sicurezza) dell'integrazione dell'IA dipende dalla capacità delle imprese di governarla come un asset industriale, e non solo come uno strumento tecnologico.

Fonte: Freepik



Il primato del Business: L'AI non deve partire dalla tecnologia, ma dalle esigenze concrete dell'azienda. La figura centrale diventa il "Business Owner", il responsabile che individua l'opportunità commerciale e se ne assume la responsabilità legale e operativa.

Architettura Organizzativa: Per un'adozione sicura, serve una struttura dedicata: una "AI Factory" per lo sviluppo tecnico, affiancata da organi di governance che definiscano regole, monitorino i rischi e gestiscano la conformità normativa.

Gestione del Rischio Preventiva: In linea con il nuovo AI Act europeo, le aziende devono cambiare paradigma. Prima di implementare un algoritmo, è necessario valutarne l'impatto sui diritti delle persone e sulla protezione dei dati, classificando i sistemi in base alla loro criticità.

Monitoraggio nel tempo: Il rischio non si esaurisce con lo sviluppo. L'articolo avverte che i modelli di AI possono "degradarsi" nel tempo o perdere affidabilità se i dati cambiano. La governance deve quindi essere un processo continuo lungo tutto il ciclo di vita del sistema.



In sintesi, l'intelligenza artificiale non può essere "esternalizzata" o delegata interamente ai tecnici. Per evitare sanzioni e garantire trasparenza, le imprese devono integrare la protezione dei dati e la conformità etica direttamente nel cuore della loro strategia aziendale.

GDPR

L'Accountability non è un'emergenza, ma un processo strategico

Il principio di accountability (o "responsabilizzazione") resta uno dei pilastri più complessi del GDPR, spesso confuso con un semplice adempimento burocratico. Un recente approfondimento di Federprivacy, a firma dell'esperta Monica Perego, chiarisce che la conformità non può essere "improvvisata" al momento di un'ispezione o di un incidente, ma deve essere costruita preventivamente attraverso una solida governance dei dati.

Inversione dell'onere della prova:

A differenza del passato, non spetta all'Autorità Garante dimostrare la violazione, ma è il titolare del trattamento a dover documentare proattivamente di aver rispettato le regole in ogni momento.

Approccio basato sul rischio:

Le misure di sicurezza non sono standard, ma devono essere modellate sulla natura e sulle finalità del trattamento. L'articolo sottolinea come l'accountability richieda tre livelli integrati: governance, gestione del rischio e documentazione probatoria

Fonte: Federprivacy



Il caso dei fornitori e dell'IA: L'articolo porta l'esempio pratico dell'onboarding di un nuovo fornitore (es. un CRM in cloud con intelligenza artificiale). Per essere "accountable", non basta firmare un contratto; serve un percorso in cinque step:

1. Qualificazione: Verificare le garanzie tecniche del fornitore (es. certificazioni ISO).
2. DPA specifico: Definire contrattualmente gli obblighi dettagliati, non limitandosi a citare il GDPR.
3. Registro dei trattamenti: Aggiornamento tempestivo delle attività.
4. DPIA: Valutare se l'uso di profilazione o IA richieda una valutazione d'impatto preventiva.
5. Audit e procedure: Monitorare costantemente l'efficacia delle misure adottate.





Euristica srl

Via Brunelleschi, snc
06024 Gubbio (PG)

www.euristica.com
privacy@euristica.com
tel. +39 075 922 1401

