

LUGLIO 2025

# NOTIZIARIO PRIVACY

PROTEGGERE I DATI,  
PROTEGGERE IL  
FUTURO

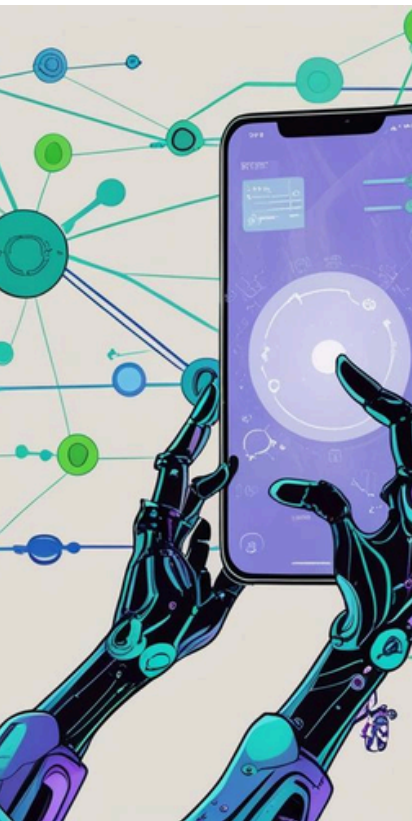
---

## 2025

WWW.EURISTICA.COM



# Table of Contents



3

**META: Al ora guarda anche nel tuo rullino?**

4

**Piattaforme digitali aziendali: il confine tra supporto e sorveglianza**

6

**Controllo indiretto e regole complesse: il caso dei metadati**

7

**Un patto per la sicurezza digitale**

8

**La vacanza dei sogni... o un incubo digitale?**

9

**L'hotel che fotocopia il tuo documento viola la privacy?**

11

**Bibliografia**

# META AI ORA GUARDA ANCHE NEL TUO RULLINO?

1



## L'ENNESIMO PASSO SILENZIOSO VERSO UN CONTROLLO SEMPRE PIÙ PROFONDO DEI NOSTRI DATI PERSONALI?

La funzione è attiva di default e non facile da disattivare. Meta afferma che le immagini non verranno archiviate né usate per addestrare l'AI, ma l'accesso ai dati è reale, il processo di opt-out è macchinoso, e le informazioni sul reale uso delle foto restano ambigue.

Solo gli ultimi 30 giorni? Forse. Alcuni suggerimenti potrebbero includere anche contenuti più vecchi, come lauree o matrimoni. Una discrepanza che alimenta il sospetto: siamo di fronte a una nuova frontiera dell'intelligenza artificiale... o della sorveglianza?

Facebook introduce una nuova intelligenza artificiale che potrà accedere automaticamente alle foto sullo smartphone per suggerire post personalizzati per eventi. Tuttavia, questa funzione solleva preoccupazioni riguardo a privacy, trasparenza e consenso<sup>1</sup>.

## “DISATTIVABILE” SÌ, MA SAI DOVE CERCARE?

Per disattivare la funzione, gli utenti devono navigare in Impostazioni -> Privacy -> Suggerimenti -> Condivisione Rullino

Fotografico: qui possono disabilitare l'elaborazione cloud, seguendo un percorso non esattamente intuitivo. Ciò ha portato alcuni a sospettare che Meta stia sfruttando la difficoltà di accesso alle impostazioni per mantenere attiva la funzionalità.

# PIATTAFORME DIGITALI AZIENDALI: IL SOTTILE CONFINE TRA SUPPORTO E SORVEGLIANZA

## Lavorare meglio... ma a che prezzo?

Sempre più aziende adottano piattaforme digitali interne per facilitare comunicazioni, richieste operative e promuovere la “consapevolezza” dei dipendenti. Sembrano strumenti neutri, persino utili. Ma cosa succede quando iniziano a tracciare ogni tuo accesso, lettura, clic o interazione?

**Non è fantascienza, ma realtà quotidiana.**

## IL QUADRO LEGALE: UNO STRUMENTO DI LAVORO... O UNA VIDEOCAMERA DIGITALE?

L'articolo 4 dello Statuto dei Lavoratori distingue tra:

Strumenti di lavoro veri e propri, usati per svolgere le mansioni (esenti da autorizzazioni)

**Strumenti che permettono un controllo a distanza**, per i quali serve accordo sindacale o autorizzazione dell'Ispettorato.

Il nodo? Capire dove finisce la “comodità” e dove inizia la “sorveglianza”.

## Il problema nascosto: tracciamento invisibile

Dietro l'interfaccia user-friendly, molte piattaforme:

- Richiedono login personali
- Registrano tempi, frequenze, contenuti visualizzati
- Generano report individuali su ciò che fai

Anche se non nascono per “spiarti”, possono farlo.  
E questo basta a far scattare l'obbligo di tutele specifiche.

## Cosa dice l'INL (e il Garante): il monitoraggio non può essere un effetto collaterale

L'ispettorato nazionale del Lavoro è chiaro: solo gli **strumenti indispensabili** al lavoro sono esenti da autorizzazioni. Se una piattaforma:

- Non è essenziale per la prestazione
- Traccia dati nominativi in modo sistematico

Allora rientra nel comma 1 e richiede l'attivazione della procedura formale

## L'autorizzazione non è un ostacolo, è una garanzia

Richiedere l'autorizzazione o firmare un accordo sindacale non significa frenare l'innovazione, ma:

- Proteggere l'azienda da contestazioni future
- Rispettare i diritti dei lavoratori
- Costruire un modello organizzativo trasparente e sostenibile

## Serve un cambio di mentalità, non di software

La vera sfida non è se usare strumenti digitali, ma **come**. Serve una valutazione preventiva e multidisciplinare – tra giuslavoristi, DPO e HR – per garantire che ogni nuova piattaforma rispetti le regole del gioco.

Perché il rischio di controllo non intenzionale esiste. E ignorarlo non è più un'opzione<sup>2</sup>.

# CONTROLLO INDIRETTO E REGOLE COMPLESSE: IL CASO DEI METADATI

## Un limite invisibile che può costare caro

21 giorni. È questo il tempo massimo che un'azienda può conservare i metadati delle email dei dipendenti senza incorrere in sanzioni, secondo il Garante della Privacy. Un termine che molti ignorano o sottovalutano, ma che può fare la differenza tra una gestione lecita e una violazione. Il caso della Regione Lombardia, sanzionata per aver trattenuto i log per 90 giorni.

## METADATI E CONTROLLI: UN EQUILIBRIO (QUASI) IMPOSSIBILE

Indirizzi email, orari, IP, dimensioni dei file: i metadati non rivelano il contenuto dei messaggi, ma dicono molto su abitudini e comportamenti dei dipendenti. Per il Garante, possono diventare strumenti di controllo indiretto e vanno quindi gestiti con attenzione.

Se usati oltre le finalità tecniche, serve un accordo sindacale o l'autorizzazione dell'Ispettorato. L'unica eccezione riguarda gli strumenti "necessari per rendere la prestazione

lavorativa". Il Garante fissa un limite di **21 giorni** per la conservazione senza autorizzazioni. Oltre, servono giustificazioni solide e documentate. Lo stesso vale per i log di navigazione web, che, se tracciano l'attività, devono essere trattati con criteri di liceità, trasparenza e proporzionalità.

Per le aziende, significa adottare informative chiare, controlli rigorosi sugli accessi e garanzie anche verso i fornitori esterni.



## Sicurezza vs privacy: un equilibrio da rivedere

Le linee guida del Garante mirano a tutelare la privacy, ma per molte aziende sono difficili da applicare, specie nei servizi cloud. Il limite dei 21 giorni non tiene conto delle esigenze reali di sicurezza informatica: attacchi o violazioni vengono spesso scoperti dopo settimane o mesi.

Così, log fondamentali per le indagini rischiano di non essere più disponibili, esponendo le organizzazioni a criticità operative e sanzioni. Servirebbe un approccio più flessibile, che bilanci privacy e sicurezza senza compromettere né l'una né l'altra<sup>3</sup>.

# UN PATTO PER LA SICUREZZA DIGITALE



## Un patto per la sicurezza digitale

Guardia di Finanza e Agenzia per la Cybersicurezza Nazionale (ACN) hanno stretto un'alleanza strategica per rafforzare la protezione cibernetica del Paese. Il protocollo punta a creare una collaborazione stabile tra le due realtà, ognuna con ruoli cruciali nella tutela degli interessi nazionali nel cyberspazio.

## FORMAZIONE, SCAMBIO DATI E RISPOSTA ALLE MINACCE

L'intesa prevede una cooperazione operativa concreta: dallo **scambio di informazioni su incidenti cyber**, alla **formazione congiunta** e alla promozione della **cultura della sicurezza informatica** presso enti pubblici e privati. Un obiettivo chiaro: **aumentare la resilienza** del sistema Paese di fronte a minacce sempre più frequenti e sofisticate.

Attraverso questo accordo, l'ACN potrà inoltre contare sulle competenze del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della GDF, che fornirà supporto investigativo e tecnico grazie alla propria esperienza nelle indagini digitali. Previsto anche l'impiego di personale qualificato del Corpo all'interno dell'Agenzia<sup>4</sup>.

## Difendersi insieme per proteggere tutti

Con questa sinergia, l'Italia compie un passo avanti nella costruzione di un ecosistema cyber più sicuro, dove la collaborazione tra istituzioni diventa uno strumento decisivo contro gli attacchi digitali. Un esempio concreto di come la sicurezza non sia solo una questione tecnica, ma anche una rete di alleanze istituzionali.

# ✈️ LA VACANZA DEI SOGNI... O UN INCUBO DIGITALE?

Anche quest'anno, nonostante l'inflazione e il caro vita, molti italiani non rinunciano alle ferie. Il 56% cerca online l'offerta più vantaggiosa, ma il pericolo è dietro l'angolo: uno su tre finisce vittima di una truffa o conosce qualcuno che lo è stato. E non si tratta di piccoli danni: il 34% dei raggiunti ha perso oltre 1.000 euro. Il rischio? Che il relax tanto desiderato si trasformi in un'amara delusione.



## 🔒 DARK PATTERN, HACKER E OFFERTE INGANNEVOLI: LA GUIDA PER DIFENDERSI

A lanciare l'allarme è il report "Safer Summer Holidays" di McAfee: oggi il 61% delle persone teme di più le minacce digitali che quelle fisiche durante i viaggi, e l'85% ha paura di subire un furto d'identità.

Il presidente Nicola Bernardi spiega: "Non si tratta più solo di virus o hacker. Gli inganni oggi sono sempre più subdoli, come grafiche ingannevoli, countdown artificiali o messaggi che ci convincono ad agire in fretta. Anche gli annunci pubblicitari personalizzati

possono mostrarci offerte più care rispetto ad altri utenti, in base al nostro profilo".

Il decalogo affronta anche il tema dei Dark Pattern, cioè quelle tecniche psicologiche che spingono l'utente a compiere scelte **contro i propri interessi**. Ad esempio? Offerte che sembrano "l'ultima disponibile" o "in scadenza" solo per creare ansia da acquisto. Il 45% degli utenti, pur sapendo di essere tracciato, cede all'impulso e compra senza leggere nulla<sup>5</sup>.

## 📅 Vacanze sì, ma con la testa

Prenotare online è comodo, ma serve attenzione. La regola d'oro? **Diffidare dalle offerte troppo belle** per essere vere, informarsi, e proteggere sempre la propria identità digitale. Una piccola precauzione in più oggi può evitare un grande rimpianto domani. Buone vacanze, ma in sicurezza.

# L'HOTEL CHE FOTOCOPIA IL TUO DOCUMENTO VIOLA LA PRIVACY?



## Check-in sì, ma con rispetto della privacy

Fotocopiare il documento d'identità all'arrivo in hotel è ancora una prassi comune, ma non sempre legale. È vero che la legge italiana (art. 109 del TULPS) impone agli hotel di identificare i clienti e comunicare le generalità alla questura. Ma questo non significa che siano autorizzati a fotocopiare o conservare il documento.

## COSA DICE IL GARANTE? MENO DATI, PIÙ RISPETTO

Il Garante italiano ha chiarito che la copia del documento può essere acquisita solo se prevista da una norma specifica. In tutti gli altri casi, è una violazione della privacy.

Anche il Garante spagnolo ha preso posizione: secondo l'AEPD, la fotocopia è una raccolta eccessiva di dati, in contrasto con il principio di minimizzazione del GDPR. Carte d'identità e patenti contengono molti più dati del necessario: foto, firma, numero, data di scadenza... tutto materiale sensibile che aumenta il rischio di **furti d'identità**.

## Lo sapevi che...?

Puoi chiedere che il tuo documento venga solo visionato e non fotocopiato.

Gli hotel devono limitarsi alla verifica visiva dell'identità. Una recente multa da 525.000 € lo conferma: una società è stata sanzionata per aver richiesto sistematicamente copie dei documenti<sup>6</sup>.

L'identificazione del cliente può avvenire tramite verifica visiva del documento, oppure, in caso di check-in online, attraverso certificati digitali, codici di autenticazione o confronto con i dati di pagamento.

**Non serve altro!**



# Bibliografia

1. *Fonte: The Verge-Note sull'Autore  
Federprivacy*
2. *Note sull'Autore Tania Orrù-  
Federprivacy*
3. *Fonte: Il Sole 24 Ore*
4. *Fonte: Agenzia per la Cybersicurezza  
Nazionale- Note sull'Autore  
Federprivacy*
5. *Note sull'Autore\_Federprivacy*
6. *Note sull'Autore\_Federprivacy*



# GRAZIE, ALLA PROSSIMA USCITA

Prepared By :  
**Euristica srl**



075 922 1401



Via Brunelleschi, snc, 06024  
Gubbio PG



[www.euristica.com](http://www.euristica.com)