

NOTIZIARIO PRIVACY

2025



INDICE

Datori di lavoro e IA

Obblighi informativi in merito all'intelligenza artificiale con la Legge 132/2025 pag 5

Azienda viola la privacy

Aggiunge il dipendente in un gruppo WhatsApp utilizzando
il suo numero privato senza consenso pag 8

PMI italiane e cyberattacchi

Il 33% delle PMI italiane ha subito almeno un cyberattacco
negli ultimi 12 mesi pag 10

Il 49% investe in cybersecurity

Solamente il 49% delle aziende che ha subito un attacco hacker
decide di investire in cybersecurity pag 12

Distinte e bonifici dei colleghi

Accesso a distinte di bonifici dei colleghi attraverso l'intranet aziendale:
illecito il trattamento dei dati personali pag 14

Autostrade per l'Italia: sanzione per 420.000€

Trattati illecitamente i dati personali di una dipendente pag 16

NOTIZIARIO PRIVACY EURISTICA
Novembre 2025

Fonte articoli
Federprivacy | federprivacy.org
Garante Privacy | www.garanteprivacy.it

Layout
Euristica

Crediti fotografici
Freepik

Euristica è iscritta a Federprivacy dal 2018



20° EVENTO FORMATIVO GRATUITO

organizzato da Euristica e rivolto a PMI, PA, liberi professionisti, lavoratori autonomi e studi professionali

Privacy come vantaggio competitivo

Scenari AI e nuove consapevolezze nelle PMI e PA

VENERDÌ | **ORE** | **HOTEL CENACOLO**
28 NOVEMBRE | **15 — 18** | **ASSISI (PG)**

→ argomenti

AI Act e privacy

L'impatto della normativa europea sull'AI e le implicazioni per la protezione dei dati personali in azienda

Deepfake e social

Le nuove tecniche di manipolazione basate su AI generativa e come difendersi

Privacy sul lavoro

Monitoraggio dipendenti, controllo remoto e geolocalizzazione, videosorveglianza

Dal Garante al Futuro

Venti anni di privacy e protezione dei dati in Italia

Case study

Provvedimento n. 451 del 4 agosto 2025 e relativo piano delle attività ispettive

→ relatori

Emanuele Florindi

Avvocato e DPO, esperto di diritto dell'informatica, bioetica e tutela dei minori

Angela Lo Giudice

Avvocato e DPO, Co-Founder di *polimeni.legal*

Gabriele Picchi

Information & cyber security manager e socio fondatore di Euristica Srl

Francesco Capparelli

Avvocato, Socio fondatore Data Intermediaries Alliance e board member Istituto Italiano Privacy

→ posti
in presenza
limitati

→ diretta
streaming

→ rilascio
attestato

→ AI PRIMI 30 ISCRITTI
in presenza in omaggio
il libro **Chat GPT: impara,
domina, crea** di Charles D. Rome

→ iscrizione
obbligatoria tramite
form sul sito
aziende.euristica.com

🌐 euristica.com
✉ info@euristica.com
☎ 075 922 1401
📱 📺 📷 📞



DATORI DI LAVORO E IA

Obblighi informativi in merito all'intelligenza artificiale con la Legge 132/2025

Con la legge 23 settembre 2025, n. 132, vengono introdotti nel nostro ordinamento nuovi principi relativi all'adozione e all'impiego dei sistemi di intelligenza artificiale.

Per quanto riguarda in particolare i datori di lavoro, l'art. 11 stabilisce che l'utilizzo dell'IA in ambito lavorativo debba essere finalizzato al miglioramento delle condizioni di lavoro, alla tutela della salute psicofisica dei dipendenti, nonché all'incremento della qualità delle prestazioni e della produttività, nel rispetto della normativa dell'Unione Europea.

L'impiego di tali tecnologie deve inoltre essere caratterizzato da sicurezza, affidabilità e trasparenza, senza poter ledere la dignità delle persone né violare la protezione dei dati personali.

Tra gli obblighi posti in capo al datore di lavoro rientra l'obbligo di informare il lavoratore in merito all'uso dell'intelligenza artificiale, secondo quanto previsto dal



decreto legislativo 26 maggio 1997, n. 152. Inoltre, in conformità al regolamento (UE) n. 2024/1689, prima dell'avvio o dell'utilizzo

di sistemi di IA ad alto rischio, il datore di lavoro è tenuto a informare i lavoratori interessati e i loro rappresentanti.

DATORI DI LAVORO E SISTEMI DI IA: PRINCIPI UE

L'art. 26, comma 7, del regolamento (UE) n. 2024/1689 stabilisce che i datori di lavoro, prima di introdurre o utilizzare sistemi di intelligenza artificiale classificati come ad alto rischio, devono informare sia i rappresentanti dei lavoratori sia i lavoratori direttamente coinvolti nell'utilizzo di tali strumenti.

Sono considerati sistemi ad alto rischio, nell'ambito della gestione del personale, quelli destinati a essere impiegati:

► **per reclutamento o selezione del personale, ad esempio nella pubblicazione di annunci mirati, nello screening delle candidature o nella valutazione dei candidati**

► **per assumere decisioni relative alle condizioni di lavoro, alla promozione o alla cessazione del rapporto, per assegnare compiti in base a caratteristiche individuali o comportamentali, o per migliorare e/o valutare prestazioni e condotte nell'ambito lavorativo.**

Se l'IA viene utilizzata anche per valutare o monitorare le prestazioni dei dipendenti, può configurarsi l'applicazione dell'art. 4 dello Statuto dei Lavoratori, che richiede una preventiva intesa con le RSA/RSU oppure, in assenza di accordo, un'autorizzazione dell'Ispettorato Nazionale del Lavoro.



OBBLIGHI INFORMATIVI A CARICO DEI DATORI DI LAVORO

L'art. 11, comma 2, della legge n. 132/2025 ribadisce che l'impiego dell'IA sul luogo di lavoro deve avvenire in modo sicuro, affidabile, trasparente e rispettoso della dignità umana e della privacy. Il datore di lavoro o il committente è pertanto tenuto a informare il lavoratore sull'impiego dell'IA, secondo le modalità previste dall'art. 1-bis del d.lgs. 26 maggio 1997, n. 152.

Ciò comporta che, qualora vengano utilizzati sistemi di IA per decisioni o monitoraggi relativi all'assunzione, gestione o cessazione del rapporto di lavoro, all'assegnazione di compiti o alla valutazione delle prestazioni e dell'adempimento degli obblighi contrattuali, il datore di lavoro deve fornire una specifica informativa, indicante:

- ambito e scopo dell'impiego dell'IA;
- processi coinvolti;
- logica di funzionamento, espressa anche con linguaggio non tecnico;
- categorie di dati trattati e tempi di conservazione;
- criteri di controllo e misure adottate;
- impatti potenziali sul rapporto di lavoro;
- livello di accuratezza, robustezza e sicurezza cibernetica dei sistemi e possibili rischi discriminatori.

Le informazioni devono essere comunicate prima dell'avvio dell'attività; eventuali modifiche significative devono essere notificate con almeno 24 ore di anticipo, come previsto dal comma 5 del medesimo articolo.



AZIENDA VIOLA LA PRIVACY

Aggiunge il dipendente in un gruppo WhatsApp utilizzando il suo numero privato senza consenso

L'Agenzia spagnola per la protezione dei dati (AEPD) ha imposto una sanzione di 70.000 euro a LVMH Iberia, S.L. (una filiale del gruppo del lusso che gestisce marchi come Louis Vuitton) per aver incluso in un gruppo di WhatsApp il numero di telefono cellulare personale di una dipendente senza il suo consenso.

La vicenda era nata dopo che una lavoratrice di LVMH si era lamentata con il garante della privacy spagnolo per il fatto che il datore di lavoro le aveva richiesto di utilizzare il suo telefono personale per lo svolgimento delle sue mansioni in attesa di ricevere un cellulare aziendale, che però non le era mai stato dato. Durante una vacanza, la dipendente aveva espressamente comunicato via email che avrebbe smesso di utilizzare il suo numero privato per questioni lavorative e aveva lasciato il gruppo WhatsApp aziendale. Tuttavia, pochi giorni dopo, il suo numero era stato nuovamente incluso in un gruppo

WhatsApp aziendale senza che lei avesse dato il suo consenso. L'azienda si era difesa sostenendo che in questi gruppi erano stati inclusi solo i dipendenti e che, di fronte alla temporanea indisponibilità dei terminali aziendali, era stato deciso di utilizzare i cellulari personali in via del tutto eccezionale per la gestione di problemi urgenti.

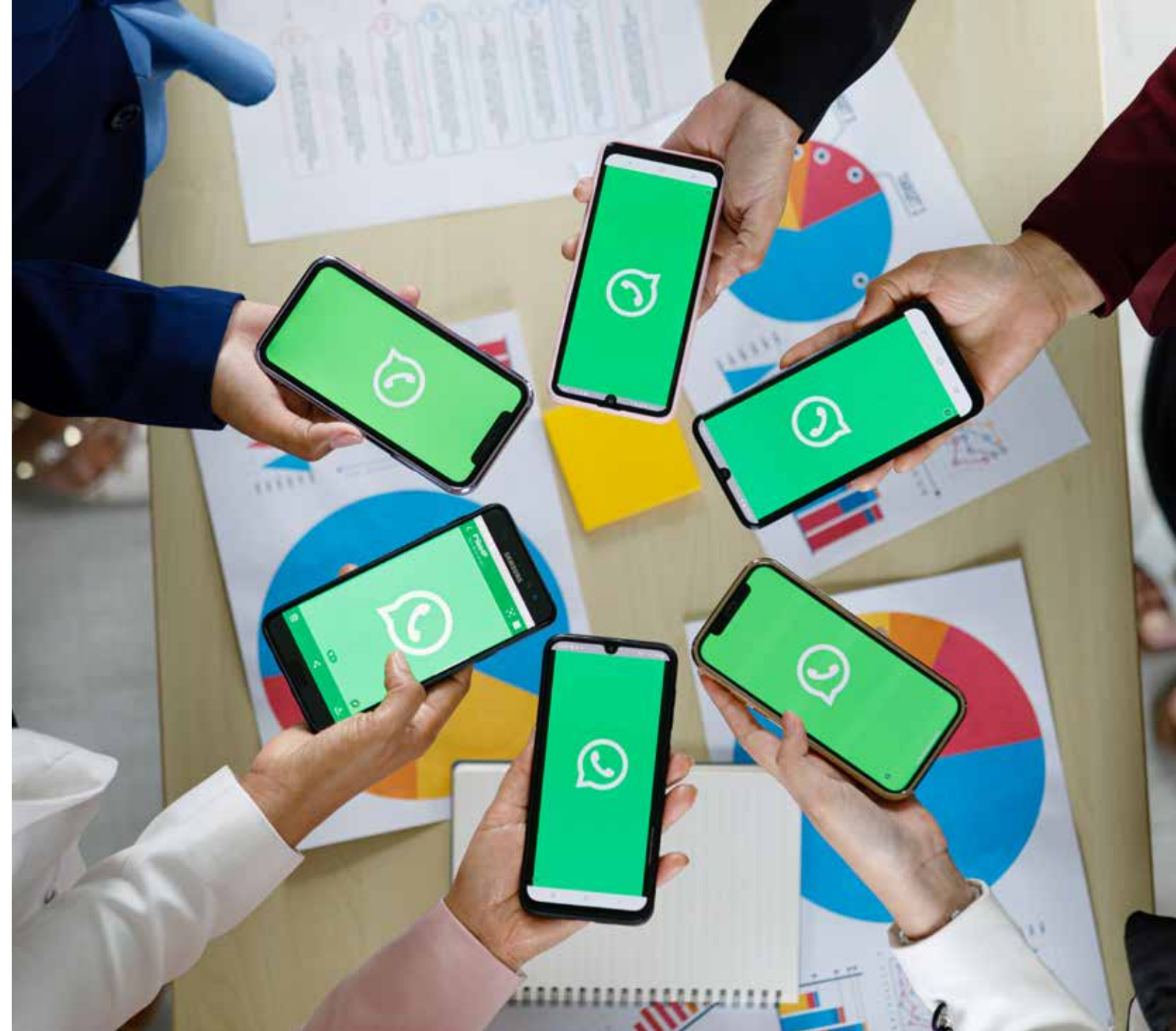
Tuttavia, l'AEPD ha ritenuto che non fosse stata stabilita alcuna base giuridica per legittimare tale trattamento dei dati. Nel suo provvedimento n. EXP202310848 l'autorità spagnola ricorda che il numero di telefono cellulare personale è un dato personale, e che il suo utilizzo per includere un lavoratore in un gruppo di messaggistica aziendale costituisce un trattamento che deve essere coperto da una qualsiasi delle basi giuridiche previste dall'articolo 6.1 del GDPR. In questo caso però non vi era stato alcun consenso dell'interessato né la necessità

contrattuale o altra motivazione legittima. Inoltre, secondo l'AEPD il fatto che la società avesse elaborato una policy interna sull'uso dei telefoni aziendali non la esenta dal rispettare l'obbligo di avere una base giuridica adeguata.

L'Autorità spagnola ha descritto l'infrazione come molto grave, e per questo aveva inizialmente proposto una multa di € 70.000, poi ridotta del 40% grazie al riconoscimento di responsabilità e del pagamento volontario di LVMH Iberia.

Oltre alla sanzione amministrativa, l'Agenzia per la protezione dei dati ha ordinato all'azienda di dimostrare l'adozione di misure a garanzia della legalità del trattamento dei dati di contatto dei dipendenti, evitando l'utilizzo di numeri personali senza consenso o senza valida base giuridica.

Fonte: Federprivacy



PMI ITALIANE E CYBERATTACCHI

Il 33% delle PMI italiane ha subito almeno un cyberattacco negli ultimi 12 mesi



Un terzo delle piccole e medie imprese italiane ha subito almeno un cyberattacco nell'ultimo anno, evidenziando una preoccupante fragilità di fronte alle minacce informatiche. A evidenziarlo è il Cisco Cybersecurity Readiness Index 2025.

Phishing, ransomware e intrusioni potenziate dall'intelligenza artificiale colpiscono sempre più spesso infrastrutture non adeguatamente protette, mentre la mancanza di risorse e la sottovalutazione del rischio amplificano la vulnerabilità complessiva.

Se il 38% delle aziende di grandi dimensioni ha affrontato un cyberattacco negli ultimi dodici mesi, secondo il report ne sono state vittima anche il 33% delle PMI italiane, che però costituiscono oltre il 90% del tessuto imprenditoriale italiano.

“Le piccole e medie imprese non possono più permettersi di sottovalutare la sicurezza informatica. Le difese di base non sono

sufficienti di fronte ad attacchi sempre più sofisticati, spesso potenziati dall'intelligenza artificiale. Un singolo attacco può bloccare le operazioni quotidiane, danneggiare la reputazione, esporre l'azienda a

conseguenze legali e, nei casi più gravi, persino portare alla chiusura dell'attività,” ha dichiarato Renzo Ghizzoni, Country Leader Sales Security di Cisco Italia.

INVESTIMENTI E PERCEZIONE DEL RISCHIO

Il rapporto di Cisco ha inoltre rilevato che solo il 21% delle PMI ha aumentato significativamente il budget per la cybersecurity negli ultimi due anni, contro il 29% delle grandi imprese.

L'aspetto più allarmante del report riguarda la percezione della propria sicurezza. Il 95% delle PMI italiane ritiene che la propria infrastruttura IT sia già adeguata a fronteggiare eventuali attacchi futuri.

Un'eccessiva fiducia che però rischia di generare un pericoloso immobilismo. “La sensazione di sicurezza diffusa tra molte PMI italiane è spesso illusoria. Troppi imprenditori sottovalutano la velocità e la sofisticazione degli attacchi informatici moderni”, osserva Ghizzoni.

CARENZA DI COMPETENZE E FRAMMENTAZIONE DELLE DIFESE

Un ulteriore elemento critico è la mancanza di personale specializzato: l'80% delle PMI segnala difficoltà nel reperire esperti di sicurezza informatica, contro il 70% delle grandi aziende. Nonostante ciò, solo un terzo delle piccole imprese intende investire in formazione o nuove assunzioni, un dato che lascia intravedere una lacuna strutturale destinata a perdurare.

A rendere il quadro più complesso contribuisce la frammentazione delle soluzioni utilizzate: il 55% delle PMI adotta tra 11 e 40 strumenti diversi per proteggersi, e il 63% dei responsabili IT ritiene che questa dispersione riduca l'efficacia complessiva della strategia di difesa. Una sicurezza distribuita su troppi livelli, spesso gestita con risorse limitate, rischia di creare più vulnerabilità che protezione.

Fonte: Federprivacy



SOLAMENTE IL 49% INVESTE IN CYBERSECURITY

La percentuale di aziende che ha subito un attacco hacker e decide di investire in cybersecurity è solo del 49%

Nella società digitale in cui viviamo gli attacchi hacker sono ormai all'ordine del giorno, eppure le imprese che ne sono colpite non corrono ai ripari per mettere in sicurezza i dati come ci si aspetterebbe, e le

ultime statistiche sembrano evidenziare pure un calo di sensibilità verso i rischi cibernetici. Se nel 2024 il 63% delle aziende che avevano subito una violazione decidevano poi di investire in cybersecurity per evitare

di trovarsi nuovamente nei guai a causa di incidenti informatici, quest'anno il rapporto "2025 Cost of a Data Breach" rivela che adesso la percentuale è scesa addirittura al 49%.

A quanto pare, meno della metà dei management che ha già sperimentato le conseguenze di un attacco informatico non sembra quindi preoccuparsi eccessivamente dell'eventualità di dover affrontare nuovamente una violazione dei dati aziendali, nonostante che lo stesso report di IBM quantifichi in 4,44 milioni di dollari il costo medio complessivo di ogni singolo "data breach".

Infatti, un'organizzazione che ha già subito un attacco hacker sa bene quanto il vortice di danni che si innesca possa risultare devastante, a cominciare dalla potenziale paralisi improvvisa delle attività produttive, l'immediata apertura di uno stato di crisi che richiede superlavoro per i propri dipendenti delle funzioni IT e Legal, spesso con la necessità di doversi avvalere anche del supporto di altri esperti e consulenti esterni specializzati con notevoli costi imprevisi.

E specialmente in ambito di intelligenza artificiale, le conseguenze di questi incidenti si riflettono direttamente sulla business continuity: secondo il suddetto rapporto, il 60% degli eventi di sicurezza ha portato alla compromissione dei dati e il 31% a vere e proprie interruzioni operative che, soprattutto per imprese di grandi dimensioni o con supply chain distribuite, incidono pesantemente sui bilanci.

Se poi i cybercriminali si servono degli ormai noti "ransomware", l'ulteriore beffa per l'azienda è quella di vedersi presentare pure il conto con una richiesta estorsiva di pagare ingenti somme di denaro per recuperare l'accesso ai dati o per evitare che questi finiscano sul Dark Web alla mercé di

malintenzionati che potrebbero utilizzarli in modo illecito per mettere in atto frodi online come furti d'identità e campagne di phishing.

Come si può ben immaginare, tutto ciò genera degli effetti a catena con enormi ripercussioni reputazionali sull'immagine dell'azienda e sulla fiducia di clienti e investitori, (a maggior ragione se la società è quotata in borsa), accompagnati dall'onere di gestire complessi adempimenti legali richiesti dal GDPR, che richiede la notifica al Garante per la protezione dei dati personali entro 72 ore dall'evento seguita da una fitta cooperazione con l'autorità in cui giocare a carte scoperte diventa una necessità per non aggravare il conto delle salatissime sanzioni previste dal Regolamento UE sulla protezione dei dati personali, che possono arrivare fino a 20 milioni di euro o al 4% del fatturato globale annuo.

Senza pensare che nei casi più gravi vi è anche l'obbligo di darne tempestivamente comunicazione ai diretti interessati coinvolti dalla violazione della loro privacy, con il probabile effetto boomerang che la notizia si diffonda sui giornali provocando una gogna mediatica con conseguenze non del tutto prevedibili che possono causare perdite di clienti e calo del fatturato.

Se purtroppo il nostro tessuto imprenditoriale fatica ancora a vedere la protezione dei dati come un investimento per proteggere i dati come un vero e proprio asset aziendale, (e a conferma di ciò un sondaggio dell'Osservatorio di Fedepriacy ha rivelato che il 78% delle imprese considera ancora il GDPR come un mero fardello burocratico), ancor peggio è constatare come purtroppo le imprese italiane non imparino la lezione neanche dopo averne pagate le conseguenze.

di Nicola Bernardi (Fonte: Economy Magazine)

DISTINTE E BONIFICI DEI COLLEGHI

Accesso a distinte di bonifici dei colleghi attraverso l'intranet aziendale: illecito il trattamento dei dati personali

Il provvedimento del Garante per la protezione dei dati personali n.490 dell'11 settembre 2025 (doc. web n. 10174501) ha deciso su un reclamo presentato da un dipendente che lamentava la diffusione indebita di dati personali propri e di altri colleghi da parte della società datrice di lavoro.

Il caso rappresenta un tipico data breach interno dovuto a errore umano nella gestione di cartelle condivise su server aziendali e offre importanti chiarimenti sull'applicazione degli artt. 5, 24 e 25 del GDPR, in relazione ai principi di accountability, minimizzazione e data protection by design e by default. Il reclamante, accedendo all'intranet aziendale da un computer condiviso, aveva potuto consultare documenti contenenti informazioni economiche e bancarie di altri dipendenti, come distinte di bonifici per trattenute stipendiali legate a prestiti, pignoramenti o cessioni del quinto. Dalle verifiche è emerso che l'evento era

dovuto a un "errore umano" dei reparti Risorse Umane e Finance, che avevano caricato file contenenti tali dati in una cartella ("SEPA") accessibile a personale non autorizzato. L'azienda ha rimosso i file entro 24 ore e aggiornato i modelli di distinta eliminando riferimenti identificativi ai dipendenti.

Nonostante le misure correttive e le giustificazioni fornite — tra cui l'avvio di una privacy gap analysis e nuove attività formative — il Garante ha ritenuto che la società avesse violato gli obblighi di sicurezza e protezione dei dati, ponendo in essere un trattamento illecito per mancato rispetto del principio di integrità e riservatezza.

Nel provvedimento, l'Autorità ha fondato la propria decisione su tre profili normativi principali del GDPR:

Art. 5, par. 1, lett. f) "Integrità e riservatezza" - I dati personali devono

essere trattati in modo da garantire un'adeguata sicurezza, anche rispetto a trattamenti non autorizzati. La disponibilità involontaria dei dati di circa 20 dipendenti in un'area accessibile a terzi costituisce violazione diretta di tale principio.

Art. 24 – Responsabilità del titolare del trattamento - Il titolare deve adottare misure tecniche e organizzative idonee a dimostrare la conformità al Regolamento. L'assenza di controlli e policy efficaci per prevenire l'accesso a documenti contenenti dati personali evidenzia una carenza di governance e supervisione del rischio privacy.

Art. 25 – Privacy by design e Privacy by default - Solo dopo l'incidente la società ha modificato i modelli eliminando i nomi dei dipendenti, segno che tali informazioni non erano necessarie alle finalità del trattamento. Il Garante sottolinea quindi

la mancata applicazione preventiva del principio di minimizzazione, e di quelli relativi alla protezione dei dati fin dalla progettazione e per impostazione predefinita.

Alla luce delle risultanze, il Garante ha dichiarato l'illiceità del trattamento, ammonito la società e disposto la pubblicazione del provvedimento sul proprio sito, oltre all'annotazione nel registro interno delle violazioni.

Il caso conferma come anche un errore apparentemente marginale nella gestione di file condivisi possa comportare gravi conseguenze sul piano del rispetto della privacy e della conformità al GDPR, ribadendo l'importanza della formazione continua e di misure organizzative proporzionate ai rischi del trattamento.

Fonte: Federprivacy





AUTOSTRADE PER L'ITALIA: SANZIONE PER 420.000€

Trattati illecitamente i dati
personali di una dipendente

Sanzione di 420mila euro del Garante privacy ad Autostrade per l'Italia Spa per aver trattato in modo illecito i dati personali di una dipendente, poi utilizzati per giustificare il licenziamento. L'intervento dell'Autorità è seguito al reclamo della lavoratrice che aveva segnalato l'utilizzo, da parte della società, di contenuti estratti dal proprio profilo Facebook e da chat private su Messenger e WhatsApp per motivare i procedimenti disciplinari a proprio carico.

Tra i contenuti utilizzati figuravano anche stralci virgolettati di commenti e descrizioni di foto. Dagli accertamenti del Garante è emerso che i contenuti erano stati utilizzati dal datore di lavoro senza una base giuridica valida, attraverso screenshot forniti da alcuni colleghi e da un soggetto terzo, presenti tra gli "amici" della dipendente su Facebook e attivi nelle sue conversazioni private su Messenger e WhatsApp. Le comunicazioni, inoltre, riguardavano opinioni e scambi avvenuti in contesti estranei al rapporto di lavoro, non rilevanti ai fini della valutazione dell'idoneità professionale.

Nel motivare la sanzione, il Garante ha sottolineato che una volta accertato il carattere privato delle conversazioni e dei commenti – pubblicati, tra l'altro, in ambienti digitali ad accesso limitato – la società avrebbe dovuto astenersi dal farne uso. L'impiego di tali informazioni, infatti, ha violato i principi di liceità, finalità e minimizzazione previsti dalla normativa privacy. L'Autorità ha inoltre ribadito che i dati personali presenti sui social network, o comunque accessibili online, non possono essere utilizzati liberamente e per qualunque scopo, solo perché visibili a una platea più o meno ampia di persone.

Anche nell'ambito dell'attività disciplinare il datore di lavoro è tenuto a bilanciare

correttamente tale potere con i diritti e le libertà fondamentali riconosciuti agli interessati. Il principio di finalità, ha ricordato l'Autorità, impone che i dati siano raccolti per scopi specifici, espliciti e legittimi, e trattati in modo coerente con tali scopi. Pertanto, l'utilizzo nel procedimento disciplinare di messaggi scambiati su canali privati di comunicazione è avvenuto in violazione della segretezza e riservatezza della corrispondenza, dunque in assenza di una giustificazione normativa.

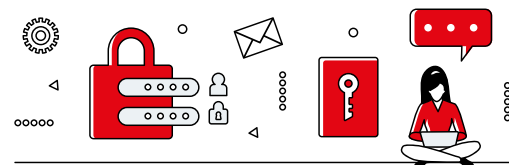
Nel determinare l'ammontare della sanzione, il Garante ha considerato sia la gravità della violazione che il fatturato della società.

Per le aziende questo provvedimento rappresenta un chiaro avvertimento: nella raccolta e uso di dati personali dei lavoratori, anche quelli "circolati" tramite social o chat private, è indispensabile rispettare la normativa privacy. Non basta che il contenuto sia visibile o reperito: è necessario che esista una base giuridica valida, che i trattamenti siano proporzionati e documentati, e che le comunicazioni riguardino solo quanto strettamente pertinente all'attività lavorativa.

Certificato Privacy è meglio

Euristica crede nella cultura della Privacy, da sempre.

Da oltre venti anni Euristica considera la cultura della Privacy uno degli asset fondamentali che ogni organizzazione deve possedere. Una cultura che non può prescindere da informazione e formazione: solo conoscendo, infatti, è possibile proteggere davvero i dati e il valore delle persone.



È per questo che nasce l'iniziativa **Certificato Privacy è meglio**

Per il 2026, lanceremo un progetto concreto per diffondere consapevolezza e competenza. 50 certificazioni professionali AICA sulla Privacy, messe gratuitamente a disposizione nel nostro parco clienti.



50

certificazioni privacy professionali



AICA

sarà l'ente certificatore



GRATIS

per i primi 50 clienti del parco Euristica



+4000€

valore complessivo dell'iniziativa

Come funziona



Le prime **50 certificazioni** sono riservate **gratuitamente** ai clienti Euristica



Raggiunte le 50, sarà possibile conseguire la certificazione **fino al 31/08/2026** con un contributo agevolato di **42 €**



L'esame si svolgerà in presenza presso la sede di **Euristica, Test Center accreditato AICA**



La certificazione viene rilasciata solo con il **superamento del 75% delle domande**

Per essere ricontattato e iscriverti all'esame

scrivici a privacy@euristica.com o vai sul sito euristica.com



EURISTICA srl

+39 075 922 1401

euristica.com

privacy@euristica.com



20 anni di Seminari Privacy, 20 anni di formazione, 20 anni insieme.

Privacy come vantaggio competitivo

VENERDÌ | **ORE** | **HOTEL CENACOLO**
28 NOVEMBRE | **15 — 18** | **ASSISI (PG)**

iscriviti al seminario gratuito su aziende.euristica.com



Euristica srl

Via Brunelleschi, snc
06024 Gubbio (PG)

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

