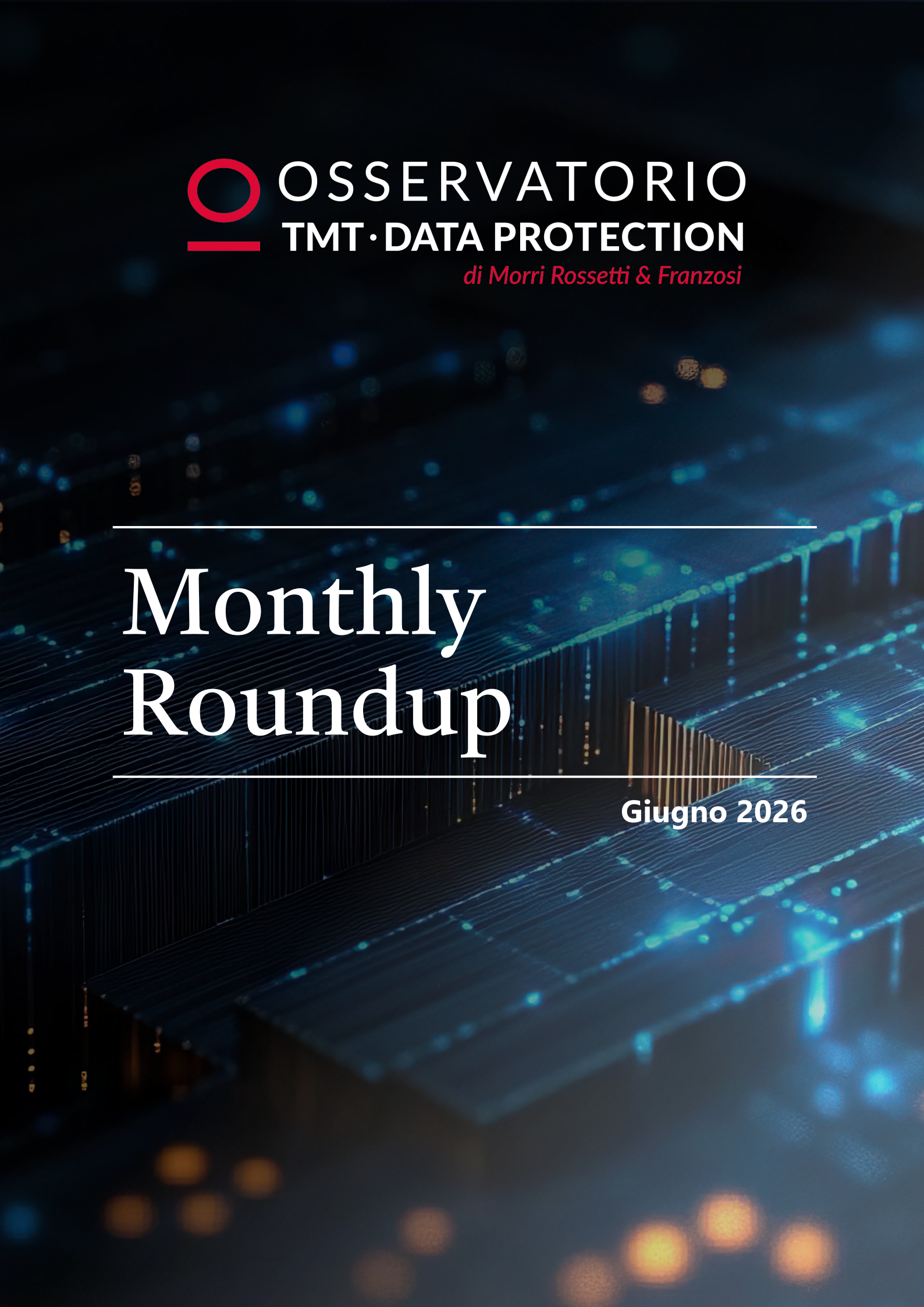


OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Giugno 2026

Giugno 2026

I principali aggiornamenti in materia di TMT & Data Protection del mese di giugno.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Passeggeri a mobilità ridotta, il Garante privacy sanziona Emirates; [Link]
- Telecamere di sicurezza urbana, Garante: usi ulteriori solo se previsti dalla legge; [Link]
- Foto dei minori sui social: serve il consenso di entrambi i genitori; [Link]
- Data breach: in consultazione il nuovo modello di notificazione approvato dai Garanti europei. [Link]

EDPB

- L'EDPB incontra il commissario dell'UE McGrath e adotta un modello comune di notifica delle violazioni dei dati; [Link]
- Supporting GDPR consistency: EDPB launches dedicated form; [Link]
- One-Stop-Shop case digest on right to object and right to erasure updated. [Link]

AGCOM

- Rapporto sull'Intelligenza Artificiale 2026. [Link]

ACN

- Aggiornate le Linee guida sulle funzioni crittografiche; [Link]
- Online l'Operational Summary di ACN di maggio. [Link]

Tracking pixel nelle e-mail: le nuove Linee Guida del Garante Privacy

È sempre più diffuso l'utilizzo di strumenti di tracciamento inseriti nelle e-mail in grado di raccogliere informazioni su comportamenti e abitudini digitali degli utenti.

La CNIL (Autorità garante francese per la protezione dei dati personali)[1] e il Garante Privacy sono recentemente intervenuti sul tema, chiarendo che anche i *pixel* di tracciamento, avendo una funzione simile ai *cookie*, devono essere letti alla luce delle regole sulla protezione dei dati personali. In particolare, il Garante Privacy ha adottato, con provvedimento n. 284 del 17 aprile 2026, le Linee Guida in materia di utilizzo di *tracking pixel* nelle comunicazioni di posta elettronica (le "**Linee Guida**").

L'obiettivo del Garante è quello di fornire a tutti i soggetti, pubblici o privati, che utilizzano *pixel* di tracciamento nelle e-mail, le corrette modalità di fornitura dell'informativa e di acquisizione del consenso *online* degli interessati.

I destinatari avranno un termine di sei mesi, a partire dal 29 aprile 2026 (data di pubblicazione delle Linee Guida in Gazzetta Ufficiale), per conformarsi alle nuove prescrizioni.

Cosa sono i *tracking pixel*?

I *pixel* di tracciamento, riconducibili alle diverse categorie di strumenti di monitoraggio digitale (come *cookie*, *script* e *widget*), sono immagini di dimensioni estremamente ridotte, spesso trasparenti e corrispondenti a un singolo *pixel*. Queste immagini non sono incorporate nell'e-mail, ma ospitate su *server* remoti.

Quando il destinatario apre il messaggio, un codice HTML genera automaticamente una richiesta al *server* del mittente, determinando il *download* del *tracking pixel* sul dispositivo dell'utente.

Attraverso questo meccanismo il mittente del messaggio o a uno dei suoi *partner* può raccogliere informazioni relative all'apertura dell'e-mail e ad altri elementi tecnici, quali l'indirizzo IP, il dispositivo utilizzato, il momento dell'apertura e il numero di visualizzazioni successive dello stesso messaggio.

La particolarità di questi strumenti risiede nella loro sostanziale invisibilità. Il destinatario non percepisce la presenza del *pixel* e, nella maggior parte dei casi, non è consapevole che l'apertura dell'e-mail stia generando una trasmissione di dati verso soggetti terzi.

Inoltre, poiché il *pixel* è generalmente associato a uno specifico destinatario, le informazioni raccolte consentono di monitorare il comportamento del singolo utente[2].

Le Linee Guida evidenziano come i *tracking pixel* siano oggi integrati nella quasi totalità delle piattaforme di e-mail *marketing*. Il loro utilizzo risponde a esigenze molto diverse: dalla verifica della corretta consegna dei messaggi al contrasto

[1] Il 14 aprile 2026 la CNIL ha pubblicato delle raccomandazioni sui pixel di tracciamento nelle e-mail.

[2] Il tracciamento ha luogo (e il pixel viene scaricato nell'e-mail dell'utente) solo nel caso in cui questi mantenga abilitata la relativa funzione di download delle immagini; se, invece, l'utente imposta la funzione di lettura dell'e-mail solo in formato testo, il tracking pixel, al pari di qualsiasi altra immagine, non sarà scaricato e dunque non potrà comportare il tracciamento del destinatario

dello *spam*, dalla misurazione delle *performance* delle campagne alla personalizzazione delle comunicazioni, fino all'identificazione di attività di *phishing*.

Proprio questa diffusione rende particolarmente rilevanti i chiarimenti forniti dal Garante, poiché l'impiego dei *tracking pixel* non interessa solo le comunicazioni commerciali e promozionali (es., *newsletter*, *direct* e-mail *marketing*), ma anche quelle di servizio o istituzionali (es., messaggi automatici, e-mail di servizio).

L'art. 122 del Codice Privacy

Il Garante Privacy qualifica l'inserimento di *tracking pixel* nelle comunicazioni elettroniche come un'ipotesi di accesso al terminale dell'utente disciplinata dall'art. 122 del Codice Privacy [3], come modificato a seguito del recepimento nel nostro ordinamento della Direttiva e-Privacy**.**

Tale norma pone un divieto generalizzato di archiviazione e accesso a informazioni nel terminale dell'utente, salvo il ricorrere di specifiche deroghe: il previo rilascio del consenso informato, libero, specifico e inequivocabile del destinatario, la necessità di effettuare la trasmissione di una comunicazione elettronica o la stretta necessità di fornire un servizio esplicitamente richiesto dall'utente.

La presa di posizione del Garante assume particolare rilievo perché estende al contesto delle comunicazioni e-mail un'impostazione già consolidata in materia di *cookie* e altri strumenti di tracciamento.

In termini pratici, il fatto che il monitoraggio avvenga attraverso un'e-mail e non durante la navigazione *web* non comporta un livello di tutela inferiore per l'interessato.

I soggetti coinvolti

L'utilizzo di *tracking pixel* può coinvolgere una pluralità di soggetti, tra cui il mittente del messaggio, il destinatario del messaggio, il fornitore di servizi di *e-mailing*, il fornitore della tecnologia di tracciamento, eventuali soggetti che mettono a disposizione liste di distribuzione e, in alcuni casi, ulteriori *partner* coinvolti nelle attività di *marketing* o analisi dei dati.

Le Linee Guida richiamano pertanto l'attenzione sulla necessità di individuare correttamente i ruoli privacy dei soggetti coinvolti, valutando caso per caso l'esistenza di rapporti di titolarità autonoma, responsabilità del trattamento o contitolarità.

Trasparenza e obblighi informativi

Secondo il Garante, l'utilizzo di *tracking pixel* può considerarsi lecito soltanto se il destinatario è preventivamente informato della loro presenza e delle relative finalità di trattamento, indipendentemente dalla natura della comunicazione o dalla tipologia del mittente.

Il punto centrale delle Linee Guida è che la trasparenza non può essere sacrificata in ragione del carattere tecnico o poco visibile dello strumento utilizzato.

Proprio perché il *tracking* avviene normalmente senza che l'utente ne abbia percezione, il rispetto degli obblighi informativi assume un ruolo determinante nella valutazione di liceità del trattamento.

[3] In particolare, il Garante Privacy sottolinea come l'inserimento di un pixel nel corpo delle e-mail e la conseguente lettura si concretizzano sia nell'archiviazione delle informazioni nell'apparecchio terminale dell'utente (inserimento del pixel di tracciamento nella e-mail), sia nel successivo accesso a informazioni già archiviate (rilevazione, tramite quel pixel, del comportamento dell'utente).

Analogamente a quanto previsto per i *cookie*[4], il Garante ammette modalità semplificate di informativa.

Le informazioni, infatti, possono essere rese su più livelli, attraverso una prima informativa sintetica accompagnata da un rinvio a quella estesa, nonché mediante canali multipli, quali canali video, *pop-up* informativi, interazioni vocali, *chatbot* o assistenti virtuali.

Per i trattamenti già in corso, le organizzazioni potranno integrare le informazioni mancanti nel primo momento utile di contatto con l'interessato. Ciò non elimina l'obbligo di adeguamento, ma consente una transizione graduale verso il nuovo assetto delineato dalle Linee Guida.

Base giuridica: quando è necessario ottenere il consenso

L'aspetto di maggiore impatto operativo riguarda l'individuazione dei casi in cui l'utilizzo dei *tracking pixel* richiede il consenso dell'interessato.

Il Garante individua alcune ipotesi nelle quali è possibile beneficiare della deroga al consenso prevista dall'art. 122 del Codice Privacy. In particolare, ciò è possibile:

- quando l'impiego di *tracking pixel* è funzionale a un conteggio statistico anonimizzato del tasso di apertura dei messaggi. In tali casi, il Garante suggerisce l'utilizzo di *pixel* identici per tutti i destinatari della medesima compagna e l'anonimizzazione degli ulteriori dati tecnici raccolti (es., indirizzo IP);
- nell'ambito di misure di sicurezza connesse ai processi di autenticazione dell'utente, come la conferma di attivazione di un *account* o la gestione di una modifica della *password*;
- nel caso di comunicazioni istituzionali o di servizio che il titolare ha l'obbligo giuridico di inoltrare (es., comunicazioni bancarie obbligatorie, notifiche di incidenti di sicurezza o campagne istituzionali informative).

La distinzione proposta dal Garante impone alle organizzazioni una valutazione preliminare sulle finalità effettivamente perseguite attraverso il tracciamento.

Se l'obiettivo è disporre di statistiche aggregate e non riconducibili ai singoli utenti, potrebbe essere possibile strutturare il trattamento in modo da rientrare nelle deroghe previste dalla normativa.

Se invece il monitoraggio è utilizzato per misurare il comportamento del singolo destinatario, ottimizzare la frequenza degli invii, segmentare il pubblico o alimentare attività di profilazione, il consenso preventivo rappresenta la regola generale.

In questo senso, le Linee Guida spingono le organizzazioni a interrogarsi sul reale valore dei dati raccolti tramite *tracking pixel* e sull'equilibrio tra benefici di *business* e oneri di *compliance*.

Per i nuovi trattamenti, il consenso dovrebbe essere raccolto preferibilmente al momento dell'acquisizione dell'indirizzo e-mail, sulla base di un'informativa adeguata e facilmente comprensibile. In un'ottica di semplificazione e per evitare fenomeni di "*consent fatigue*", il Garante ammette che il consenso all'utilizzo dei *tracking pixel* possa essere ricompreso in quello, più generale, relativo alla ricezione delle comunicazioni promozionali, purché la richiesta

[4] *Cfr*. Garante Privacy, Linee guida cookie e altri strumenti di tracciamento – 10 giugno 2021.

sia formulata in modo chiaro, neutro e non condizionante.

Particolare attenzione dovrà essere dedicata ai meccanismi di revoca. Gli utenti devono poter revocare in modo agevole e granulare le proprie scelte, sia interrompendo del tutto la ricezione delle comunicazioni, sia continuando a ricevere quelle prive di *pixel*, senza essere sottoposti ad attività di tracciamento.

Per i trattamenti già in essere alla data di entrata in vigore delle Linee Guida, è previsto un regime transitorio. Dopo aver adempiuto agli obblighi informativi, il titolare dovrà implementare e rendere disponibile un meccanismo che consenta la revoca del consenso, anche in forma granulare.

Conclusioni

Le nuove Linee Guida impongono alle organizzazioni di considerare i *tracking pixel* non più come una funzionalità tecnica accessoria, ma come un trattamento che richiede una specifica valutazione sotto il profilo privacy.

Il tema non è soltanto giuridico. Le nuove regole potrebbero incidere direttamente sui principali indicatori utilizzati per misurare l'efficacia delle campagne e-mail, sui processi di segmentazione del pubblico e sulle strategie di personalizzazione delle comunicazioni.

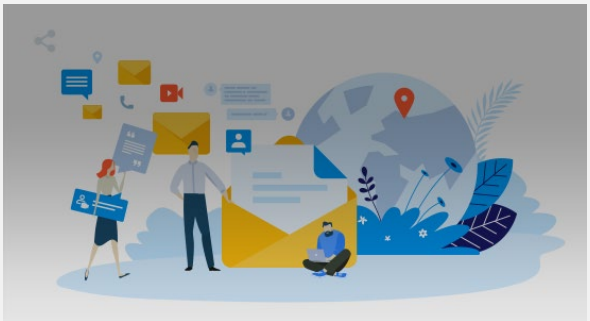
Nei sei mesi concessi dal Garante per l'adeguamento, sarà opportuno verificare:

- quali flussi di comunicazione e-mail prevedano l'utilizzo di *tracking pixel*;
- quali siano le finalità perseguite;
- se le informative privacy necessitino di un aggiornamento;
- se i meccanismi di raccolta e revoca del consenso risultino conformi alle indicazioni del Garante;
- se le piattaforme tecnologiche utilizzate consentano una gestione effettiva e granulare delle preferenze degli interessati;
- se sia necessario adottare ulteriori misure tecniche e organizzative ispirate ai principi di *privacy by design* e *by default*[5].

Le organizzazioni che affronteranno tempestivamente queste verifiche potranno ridurre il rischio di non conformità e, al contempo, costruire modelli di comunicazione più trasparenti e sostenibili nel lungo periodo.

* * *

Sistemi di AI per l'analisi dello stress dei lavoratori: il caso Myndoor



Può un'impresa mettere a disposizione dei propri dipendenti uno strumento di IA capace di analizzare il livello di stress attraverso le conversazioni su Teams o Slack? E, soprattutto, quali verifiche deve svolgere prima di adottare una tecnologia di questo tipo?

[5] In tale ottica, il Garante menziona le soluzioni volte a ridurre i rischi di identificazione degli interessati come, ad esempio, la generazione di un identificativo inintelligibile e non sequenziale da associale all'indirizzo e-mail dell'utente, mantenendo tale corrispondenza in un layer interno e separato dalla piattaforma utilizzata.

Il provvedimento del Garante Privacy del 14 maggio 2026 offre una prima risposta a queste domande. Pur riguardando il caso di Myndoor S.r.l. ("**Myndoor**" o la "**Società**"), la decisione contiene indicazioni che interessano tutte le organizzazioni che intendano introdurre strumenti di IA destinati al benessere organizzativo, alla gestione delle risorse umane o, più in generale, al contesto lavorativo.

L'aspetto più significativo del provvedimento, infatti, non riguarda tanto la liceità del singolo applicativo: il Garante concentra l'attenzione sui possibili effetti che il suo utilizzo potrebbe produrre nell'organizzazione aziendale e sui rischi che potrebbero derivarne per i diritti dei lavoratori.

Il caso Myndoor

Con il proprio provvedimento, il Garante Privacy ha rivolto un ammonimento a Myndoor, *start-up* italiana che ha sviluppato un *plug-in* integrabile in Microsoft Teams e Slack, destinato ad analizzare, mediante tecniche di IA e analisi semantica, il livello di stress psicologico dei lavoratori che decidano volontariamente di utilizzarlo.

L'istruttoria è stata avviata d'ufficio a seguito di alcune notizie di stampa che riferivano dell'utilizzo del sistema presso enti pubblici. Nel corso degli accertamenti, tuttavia, la Società ha chiarito che l'ente inizialmente indicato non aveva acquistato il servizio, non avendo quindi trattato i dati dei propri dipendenti in qualità di datore di lavoro.

Venuto meno tale presupposto, il Garante ha progressivamente spostato il proprio esame dal caso concreto alle modalità con cui il sistema potrebbe essere utilizzato, in futuro, da imprese ed enti che decidessero di adottarlo.

Proprio questo passaggio rende il provvedimento particolarmente interessante: pur in assenza di un utilizzo effettivo da parte di un datore di lavoro, il Garante individua alcuni profili di rischio che, secondo l'Autorità, dovrebbero essere affrontati già nella progettazione del servizio e prima della sua diffusione sul mercato.

Come funziona il *plug-in* Myndoor?

Il lavoratore che lo desideri può attivare il *plug-in* affinché i contenuti testuali dei messaggi scambiati su Teams o Slack vengano analizzati da un modello di IA che ne stima i parametri di stress, restituendo all'interessato suggerimenti e indicazioni per il benessere personale.

Il datore di lavoro non può accedere né ai contenuti delle conversazioni né ai risultati delle analisi riferibili ai singoli dipendenti. Tuttavia, è prevista la possibilità che il datore richieda un *report* settimanale contenente dati aggregati sul livello di stress della popolazione aziendale, purché vi siano almeno dieci utenti attivi.

La qualificazione dei ruoli privacy

Il Garante osserva che il rapporto relativo al trattamento dei dati si instaura esclusivamente tra Myndoor e i lavoratori che abbiano scelto di utilizzare il servizio. In tale relazione la Società opera quale titolare del trattamento.
La conclusione è significativa perché il servizio viene comunque acquistato dal datore di lavoro.

L'impostazione richiama quella già seguita per altri servizi messi a disposizione dei dipendenti nell'ambito delle politiche di *welfare* aziendale, come le assicurazioni sanitarie o altre prestazioni erogate da soggetti terzi. Anche in tali ipotesi il datore sostiene economicamente il servizio senza entrare nella disponibilità dei dati personali trattati dal fornitore.

Il rischio di re-identificazione

Il principale profilo di attenzione individuato dal Garante riguarda la possibilità per il datore di lavoro di richiedere un *report* aggregato contenente informazioni sul livello di stress dei dipendenti che utilizzano il servizio.

In astratto, il *report* non contiene dati riferibili ai singoli lavoratori. Tuttavia, il provvedimento evidenzia come l'aggregazione dei dati non rappresenti, di per sé, una garanzia sufficiente. In determinati contesti organizzativi – soprattutto nelle realtà di dimensioni ridotte o caratterizzate da gruppi di lavoro facilmente individuabili – anche informazioni presentate in forma statistica potrebbero consentire di formulare inferenze sui singoli interessati.

L'attenzione dell'Autorità si concentra, quindi, non tanto sul dato aggregato in sé, quanto sul rischio che quest'ultimo possa essere combinato con altre informazioni già nella disponibilità del datore di lavoro, rendendo possibile, anche indirettamente, l'identificazione dei lavoratori che abbiano aderito al servizio.

Per tali ragioni, il Garante ha invitato Myndoor a adottare, nel rispetto dei principi di *privacy by design* e *by default*, misure e accorgimenti intesi a prevenire qualsiasi forma di messa a disposizione, anche mediante il *report*, dei dati dei dipendenti che decidano di fruire del *plug-in*. L'obiettivo è evitare che i datori di lavoro, anche in via indiretta, vengano a conoscenza delle informazioni trattate mediante tale sistema.

Le implicazioni sul piano giuslavoristico

Il Garante ribadisce che le informazioni relative allo stato emotivo, al livello di stress o, più in generale, al benessere psicologico del lavoratore appartengono a una sfera che l'ordinamento sottrae alla disponibilità del datore di lavoro (*cfr*. art. 113 del Codice Privacy, che rinvia alle disposizioni a tutela della dignità della persona e al divieto di raccolta di dati non pertinenti all'attività lavorativa di cui allo Statuto dei Lavoratori e alla Legge Biagi).

Questa tipologia di informazioni non può infatti costituire oggetto di conoscibilità da parte del datore di lavoro, né direttamente né attraverso forme di aggregazione idonee a consentire inferenze individuali.

L'Autorità attribuisce inoltre rilievo alla circostanza che, nell'informativa privacy predisposta da Myndoor, il servizio venga ricondotto a finalità di medicina preventiva, diagnosi e assistenza.

Da tale qualificazione deriva un'ulteriore conseguenza: qualora il sistema svolga una funzione riconducibile all'accertamento dello stato di salute del lavoratore, ogni valutazione resta riservata al medico competente, senza che il datore possa acquisire direttamente le relative informazioni[6].

Il richiamo all'AI Act

Tra i passaggi più interessanti della decisione vi è il richiamo all'art. 5, paragrafo 1, lettera f), dell'AI Act, che vieta, in linea generale, l'immissione sul mercato, la messa in servizio o l'uso di sistemi di intelligenza artificiale destinati a inferire le emozioni delle persone nei luoghi di lavoro, salvo le eccezioni previste dallo stesso Regolamento (i.e. finalità mediche o di sicurezza)[7].

[6] *Cfr*. Documento di indirizzo del Garante Privacy sul ruole del medico competente (Provvedimento del 13 maggio 2021, doc. web., 958536).

[7] Tale eccezione, proprio perché incide su un divieto posto a presidio della dignità e dell'autodeterminazione della persona, deve tuttavia essere interpretata in modo rigoroso, documentata ex ante e circoscritta allo stretto necessario.

Nel caso di specie, tuttavia, il sistema sviluppato da Myndoor opera attraverso l'analisi semantica di testi liberamente digitati dagli utenti e non mediante il trattamento di dati biometrici [8], ai quali il divieto dell'AI Act espressamente si riferisce.

Il richiamo al divieto previsto dall'AI Act sembra assumere, in questo contesto, una funzione principalmente sistematica.

Da un lato, esso rafforza le conclusioni raggiunte dal Garante in materia di protezione dei dati personali, nella misura in cui l'Autorità evidenzia l'esigenza di evitare che sistemi di questo tipo possano tradursi, anche indirettamente, nella messa a disposizione del datore di lavoro di informazioni inferite mediante tecniche di IA sullo stato psicologico dei dipendenti.

Dall'altro lato, il riferimento all'AI Act consente di richiamare alcuni limiti strutturali delle tecnologie di intelligenza artificiale, tra cui la ridotta trasparenza e spiegabilità degli *output*, il rischio di *bias* e di risultati discriminatori e la necessità di garantire un controllo umano effettivo sull'utilizzo del sistema.

Più che sul divieto in sé, l'attenzione si sposta quindi sulle concrete modalità di impiego del sistema all'interno dell'organizzazione. In particolare, occorre verificare se lo strumento possa essere utilizzato per monitorare, anche indirettamente, le prestazioni o il comportamento dei lavoratori, con la conseguenza di ricondurlo potenzialmente nell'ambito dei sistemi di IA ad alto rischio.

Per tali sistemi, come richiamato dallo stesso provvedimento del Garante, l'AI Act prevede che il fornitore metta a disposizione dei deployer informazioni adeguate sulle finalità previste, sul livello di accuratezza, robustezza e cybersicurezza, sui rischi per la salute e la sicurezza e per i diritti fondamentali, nonché sulle caratteristiche tecniche del sistema[9].

Si tratta di informazioni che le imprese dovrebbero esaminare già nella fase di selezione del fornitore, poiché costituiscono il presupposto per valutare se il sistema possa essere utilizzato in modo conforme all'interno della propria organizzazione.

Conclusioni

Alla luce delle indicazioni che emergono dal provvedimento, il tema centrale non riguarda soltanto la conformità del singolo sistema di IA, ma il momento in cui tale conformità viene effettivamente verificata.

Il caso Myndoor mostra infatti come le principali criticità non emergano necessariamente dall'utilizzo in concreto dello strumento, quanto piuttosto dalla sua progettazione, dalla configurazione dei flussi di dati e dalle modalità con cui esso viene inserito nei processi aziendali.

Come specificato nelle Linee Guida della Commissione europea sulle pratiche vietate di intelligenza artificiale (4 febbraio 2025), tale eccezione deve essere intesa in modo restrittivo, essendo applicabile solo in relazione alla protezione della vita e della salute e non alla protezione di altri interessi (ad es., protezione dei beni da furti e truffe).

[8] Si tratta, cioè, di dati ricavati da uno specifico trattamento tecnico relativi a caratteristiche fisiche, fisiologiche o comportamentali, come le immagini facciali o le impronte digitali.

[9] L'Art. 13 dell'AI Act, in particolare, prevede che i sistemi di IA ad alto rischio devono essere progettati in modo sufficientemente trasparente da consentire ai deployer di comprendere e interpretare correttamente gli output prodotti. A tal fine, il fornitore deve fornire istruzioni d'uso chiare e complete contenenti, tra le altre, informazioni sulle finalità, le capacità e le caratteristiche tecniche del sistema, sui livelli di accuratezza, sui rischi prevedibili, sulle misure di sorveglianza umana e sui requisiti necessari al corretto funzionamento del sistema.

In questo senso, l'adozione di sistemi di IA nel contesto lavorativo richiede un passaggio preliminare: la valutazione del caso d'uso e del fornitore.

Non si tratta soltanto di verificare se lo strumento sia formalmente conforme alla normativa applicabile, ma di comprendere quali dati vengano trattati, con quali logiche di elaborazione, quali informazioni possano essere inferite e quali effetti il suo utilizzo possa produrre sull'organizzazione del lavoro e sui lavoratori.

Su questo piano, il provvedimento del Garante evidenzia alcuni profili che le imprese dovrebbero considerare con particolare attenzione prima dell'introduzione di strumenti analoghi:

- la possibilità che informazioni apparentemente aggregate possano, in determinati contesti, tradursi in inferenze individuali;
- il rischio che sistemi progettati per finalità di supporto al benessere organizzativo possano incidere, anche indirettamente, su dinamiche di controllo o valutazione del personale;
- la necessità di comprendere in anticipo la qualificazione del sistema ai sensi dell'AI Act e gli obblighi informativi che ne derivano per il fornitore.

Ne deriva che la conformità dei sistemi di IA non può essere gestita come una fase successiva all'adozione dello strumento, ma deve essere integrata nel processo decisionale che conduce alla sua scelta.

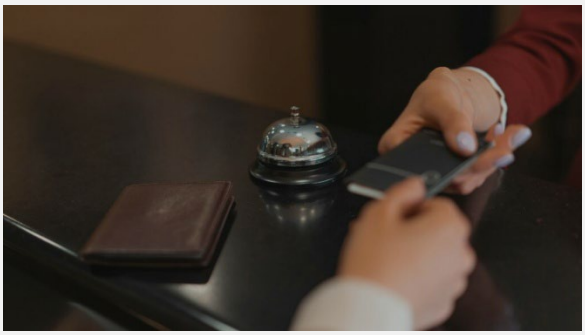
È in quel momento che l'impresa è chiamata a valutare se il sistema sia effettivamente compatibile con il proprio contesto organizzativo e con il quadro normativo applicabile, tenendo conto non solo delle funzionalità dichiarate dal fornitore, ma anche degli utilizzi ragionevolmente prevedibili.

Per questo motivo, la selezione del fornitore e la valutazione preventiva del sistema assumono un ruolo centrale nella *governance* dell'IA in ambito lavorativo.

Una decisione informata in questa fase consente non solo di ridurre il rischio giuridico, ma anche di evitare che strumenti pensati per finalità di supporto si traducano, nella pratica, in meccanismi di monitoraggio o di gestione del personale non coerenti con i limiti posti dall'ordinamento.

* * *

Privacy e strutture ricettive: i chiarimenti del Garante Privacy sulla conservazione dei documenti degli ospiti



Quando una struttura ricettiva effettua il *check-in* di un ospite, la copia del documento di identità viene spesso acquisita e archiviata quasi automaticamente.

È una prassi diffusa, incorporata nei processi operativi di molti hotel, B&B e affittacamere, talvolta attraverso procedure cartacee, talvolta tramite *software* che conservano immagini dei documenti all'interno dei sistemi gestionali.

La recente nota di chiarimento del Garante Privacy offre però un'indicazione che molte strutture potrebbero trovare meno scontata di quanto sembri: l'obbligo di identificare gli ospiti

e comunicarne i dati all'Autorità di pubblica sicurezza non autorizza la conservazione delle copie dei documenti di identità.

Per anni molte strutture hanno considerato la conservazione della copia del documento come una naturale estensione dell'adempimento previsto dalla normativa di pubblica sicurezza.

In realtà, i due piani sono distinti: una cosa è raccogliere i dati necessari per effettuare la comunicazione prevista dalla legge; altra cosa è mantenere nel tempo una copia integrale del documento.

La questione non è soltanto formale. La conservazione delle immagini dei documenti rappresenta oggi uno dei principali fattori di esposizione al rischio privacy per il settore alberghiero.

Carte d'identità, passaporti e altri documenti contengono infatti un insieme di informazioni particolarmente appetibili in caso di accesso abusivo, furto di dati o utilizzo fraudolento delle credenziali di accesso ai sistemi informatici della struttura.

Per questo motivo il chiarimento del Garante va letto come un invito a ripensare i processi di raccolta dei dati secondo il principio di minimizzazione: se la finalità è adempiere all'obbligo di comunicazione previsto dalla legge, la conservazione della copia del documento richiede una giustificazione autonoma che, nella maggior parte dei casi, non esiste.

Cosa prevede la normativa

La disciplina di pubblica sicurezza (art. 109 TULPS) impone ai gestori delle strutture ricettive di comunicare alle Autorità di pubblica sicurezza le generalità degli ospiti attraverso il sistema "Alloggiati Web", secondo le modalità stabilite dal Ministero dell'Interno[10] L'obiettivo sotteso è quello di assicurare la tutela dell'ordine e della sicurezza pubblica e prevenire e reprimere fenomeni criminali.

Proprio per questa ragione, l'obbligo previsto dalla legge riguarda la comunicazione dei dati, non la conservazione delle copie dei documenti presso la struttura.

Il Garante richiama espressamente il quadro normativo di riferimento, evidenziando che, una volta effettuata la trasmissione tramite il sistema "Alloggiati Web" e ottenuta la relativa ricevuta, eventuali copie dei documenti acquisite per effettuare l'adempimento devono essere cancellate o distrutte.

Si tratta di un passaggio che molte organizzazioni tendono a sottovalutare. Nella pratica, infatti, il documento viene spesso acquisito una prima volta per estrarre i dati necessari alla comunicazione e una seconda volta attraverso la sua conservazione nei sistemi interni. Ed è questo secondo momento a generare il problema.

I processi digitali di *check-in*

L'aspetto probabilmente più interessante del chiarimento riguarda le modalità con cui oggi vengono gestiti i *check-in*. Sempre più strutture utilizzano *Property Management System*, applicazioni per il *self check-in* o procedure che consentono agli ospiti di caricare preventivamente una fotografia del documento. In molti casi tali strumenti conservano automaticamente l'immagine acquisita, creando

[10] *Cfr*. decreto del Ministro dell'Interno del 7 gennaio 2013 recante "*Disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive*", come modificato dal decreto del Ministro dell'Interno del 16 settembre 2021, già oggetto di provvedimento del Garante (provvedimenti n. 295 del 18 ottobre 2012, doc. web n. 2099252, e n. 300 dell'8 luglio 2021, doc. web n. 9690786).

archivi che possono accumulare migliaia di documenti nel tempo.

Da una prospettiva di protezione dei dati, il rischio non deriva tanto dall'acquisizione iniziale dell'immagine, quanto dalla sua permanenza nei sistemi informatici della struttura o dei fornitori tecnologici coinvolti nel processo.

La domanda che gli operatori dovrebbero porsi non è quindi se il *software* consenta di acquisire il documento, ma se sia configurato per eliminarlo una volta esaurita la finalità di identificazione e completata la comunicazione alle Autorità. In molti casi, una verifica dei flussi applicativi e delle impostazioni di conservazione può rivelare criticità che passano inosservate per anni.

I rischi sottesi alla prassi di conservare le copie dei documenti

Il problema non è teorico. Le copie dei documenti di identità rappresentano uno dei *dataset* più sensibili nel settore *hospitality*, perché contengono un insieme di informazioni che, se sottratte, possono essere immediatamente riutilizzate per furti di identità o frodi documentali.

Queste prassi, oltre a non trovare fondamento normativo, moltiplicano i punti di rischio. Negli ultimi anni diversi episodi di *data breach* nel settore[11] hanno avuto proprio questo tipo di origine: archivi non necessari, conservati per comodità operativa più che per reale esigenza giuridica.

Il Garante, infatti, ha registrato un aumento considerevole dei reclami, delle segnalazioni e dei quesiti riguardanti la raccolta dei dati contenuti nei documenti di identità degli ospiti delle strutture ricettive (ad es., tramite foto o documenti inviati tramite WhatsApp).

I chiarimenti del Garante Privacy

a. **Base giuridica e periodo di conservazione**

Secondo il Garante, il trattamento dei dati effettuato per l'identificazione degli ospiti trova la propria base giuridica nell'adempimento di un obbligo legale cui è soggetto il titolare del trattamento. Tale obbligo, tuttavia, si esaurisce nella comunicazione dei dati all'Autorità competente.

La normativa di pubblica sicurezza non impone, come visto, la conservazione delle copie dei documenti presso la struttura ricettiva e non può quindi essere invocata per giustificare archivi documentali permanenti. L'unico documento che deve essere conservato (per 5 anni) è la ricevuta rilasciata dal sistema "Alloggiati Web", che attesta l'avvenuta trasmissione dei dati.

b. **Misure di sicurezza**

Il Garante richiama inoltre l'obbligo, previsto dal GDPR, di adottare misure tecniche e organizzative adeguate per la protezione dei dati personali trattati.

Ciò significa che le strutture ricettive devono prestare particolare attenzione alle modalità con cui il personale raccoglie i dati degli ospiti e alle configurazioni dei sistemi utilizzati per la gestione dei *check-in*.

Una procedura conforme sulla carta può infatti diventare non conforme se il *software* continua a conservare automaticamente le immagini dei documenti.

[11] Per maggiori approfondimenti, si veda il nostro precedente contributo "*Data breach negli hotel: obblighi, rischi e tutele*"

c. ***Data breach***

In caso di violazione dei dati personali che coinvolga copie di documenti d'identità, il rischio per gli interessati può essere particolarmente elevato. Per questo motivo il Garante ricorda che, qualora si verifichi un *data breach* possono sorgere gli obblighi di notifica all'Autorità entro 72 ore e, nei casi più gravi, di comunicazione della violazione agli interessati.

Cosa devono fare in concreto le strutture ricettive?

Alla luce dei chiarimenti forniti dal Garante e tenuto conto che l'attività ricettiva comporta ogni anno il trattamento dei dati personali di milioni di persone, le strutture ricettive dovranno:

- formare adeguatamente e responsabilizzare il personale addetto al *check-in*, fornendo istruzioni chiare sul divieto di conservare copie (analogiche o digitali) dei documenti una volta completati gli adempimenti di legge;
- aggiornare le informative privacy, chiarendo agli ospiti le modalità di trattamento dei dati e l'assenza di una conservazione sistematica delle copie dei documenti;
- disciplinare correttamente i rapporti con i fornitori dei servizi di gestione delle prenotazioni alberghiere e dei servizi eventualmente utilizzati per l'acquisizione dei dati relativi ai documenti di identità, nominandoli responsabili del trattamento *ex* art. 28 del GDPR;
- evitare di raccogliere i documenti d'identità tramite fotografie scattate con dispositivi mobili o l'invio attraverso applicazioni di messaggistica quali WhatsApp.

Per molte strutture la questione non richiederà investimenti significativi, ma una verifica critica delle modalità con cui vengono gestiti i documenti degli ospiti.

In un contesto in cui i *data breach* rappresentano un rischio sempre più concreto, ridurre la quantità di dati conservati non è soltanto una misura di conformità, ma una misura di riduzione dell'esposizione a rischi legali, operativi e reputazionali.

Per maggiori informazioni e approfondimenti

Carlo Impalà
Partner e Responsabile Osservatorio TMT&DP

Carlo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it