QUOTIDIANOPIÙ

Lunedì 13/07/2026 • 05:00

LAVORO VERSIONE ITALIANA

Accesso dell'ex dipendente agli strumenti aziendali: eccessi di tutela?

Il **Garante Privacy** sanziona un'azienda per le modalità con cui era stato consentito l'**accesso di un ex dipendente a mail e file personali**: un provvedimento forse eccessivo, ma che offre spunti su **policy interne**, **tempi di conservazione** e **gestione proattiva** delle richieste di accesso.

di Luca Failla - Avvocato Managing Partner Failla&Partners Studio Legale

di Paola Salazar - Avvocato in Milano

L'evoluzione tecnologica in atto, accompagnata dall'evoluzione degli orientamenti in materia di **controlli e di tutela della privacy** sta iniziando a generare nuove complessità nella gestione del **rapporto di lavoro**. La normativa europea e nazionale in materia di intelligenza artificiale,

- Reg. UE 1689/2024 (e Pacchetto Omnibus di semplificazioni) da un lato;
- e L. 132/2025 e relativi decreti attuativi dall'altro;

introducono obblighi di **adeguamento tecnico e organizzativo** e regole di compliance che si intrecciano necessariamente con la disciplina del **GDPR** (Reg. UE 2016/679) e con gli orientamenti ed i provvedimenti del **Garante Privacy nazionale**.

In questo scenario, se tale complessa regolazione porta da ultimo la Cassazione a riconoscere l'**utilizzabilità dei dati raccolti** attraverso specifici strumenti tecnici (quali il ***badge***, su cui v. da ultima Cass. 7985/2026), dall'altro porta invece da tempo il Garante a **restringere sempre di più gli spazi** per il legittimo esercizio dei **poteri organizzativi** all'interno delle aziende.

Laddove appare legittimo limitare l'uso di strumenti diretti a creare forme di controllo occulto, specie oggi se integrati da applicativi che sfruttano l'AI (su cui cfr. il Provvedimento 14 maggio 2026 n. 342), per contro non si comprendono le ragioni del **particolare rigore** con cui viene spesso sanzionato l'**esercizio del potere direttivo ed organizzativo sugli strumenti di lavoro**.

Accesso a casella e-mail e file personali per l'ex dipendente

L'ultimo esempio è il Provvedimento 12 marzo 2026 n. 165 con il quale il Garante è tornato ad esprimersi in materia di accesso ai dati ed in particolare in merito all'accesso – su richiesta di un lavoratore - ai documenti e alle **cartelle personali presenti sul proprio PC aziendale** e nella casella di **posta elettronica aziendale**.

La questione nel caso specifico gravitava soprattutto intorno alle modalità di conservazione dei documenti e dei dati personali dei lavoratori. In questo campo, quello che ormai conta prioritariamente per il Garante è la **commistione tra dati personali e dati aziendali** qualora emergano esigenze di accesso ai dati personali in relazione ai quali gli obiettivi di tutela finiscono per attrarre anche le modalità di gestione dei dati aziendali.

Il provvedimento nasceva dalla richiesta di un ex dipendente, il quale, a seguito della cessazione del rapporto di lavoro, chiedeva l'accesso al desktop e alla posta elettronica per il recupero dei documenti personali. Sulla base di tali richieste, la società organizzava così una serie di incontri in presenza diretti ad **affiancare il lavoratore nell'acquisizione dei dati richiesti**, provvedendo così a consegnare in primo luogo la posta elettronica personale e successivamente anche la documentazione inerente il rapporto di lavoro. Documentazione che veniva debitamente **anonimizzata** relativamente ai dati personali attinenti a soggetti terzi, ma della quale il lavoratore contestava il merito, considerandola di fatto "*epurata di molti elementi*". Con la cessazione del rapporto di lavoro, la società aveva tra l'altro provveduto alla **disattivazione della casella di posta elettronica** - con reindirizzamento previsto per 14 giorni – per poi provvedere alla successiva cancellazione dell'account previo backup a fini di conservazione dei dati aziendali (prevista per 5 anni).

Dopo un'analisi dei fatti, tenendo conto della richiesta di accesso formulata dal lavoratore, delle modalità di evasione della richiesta e soprattutto dei tempi previsti per la conservazione dei dati previsti (5 anni per il backup della casella e 12 mesi per i metadati di navigazione) il Garante ha dichiarato la condotta del datore di lavoro illecita, irrogando apposita sanzione. Ritiene infatti l'Autorità che l'attività di **esame preventivo delle e-mail** contenute nella casella di posta, messa in pratica dall'azienda, nonché il successivo oscuramento, abbia comportato un **pregiudizio ai diritti e libertà del lavoratore** in materia di accesso ai dati, a nulla rilevando la difesa della società di aver agito (prioritariamente) a **tutela dei dati aziendali**, anche al fine di scongiurare la diffusione di segreti aziendali. Il Garante sostiene nel provvedimento che il **titolare del trattamento** dovrebbe

essere in grado, in situazioni di questo tipo, di poter **dimostrare** che le limitazioni al diritto di accesso sono giustificate da **legittimi presupposti organizzativi** legati anche alla necessità di non pregiudicare i diritti e le libertà di soggetti diversi dall'interessato, sottolineando come in questi casi il diritto di accesso possa essere limitato solo in caso di richieste manifestamente infondate o eccessive.

***Ratio* della decisione e spunti operativi**

In definitiva, il Garante muove i suoi passi proprio dalla **nozione di "trattamento"** definita all'art. 4 del GDPR, dentro la quale rientra anche la conservazione e l'organizzazione dei dati. Vengono poi in considerazione, gli artt. 13, 14 e 15 GDPR che richiedono la predisposizione di una idonea informativa sulle modalità e finalità di trattamento dei dati, tenendo conto del **principio di minimizzazione**, quindi di un tempo di conservazione delle informazioni proporzionato ed adeguato rispetto al suo scopo. Ed è in questa cornice che i datori di lavoro devono trovare il proprio spazio per definire le più adeguate misure tecniche di gestione dei dati e per trovare le soluzioni organizzative più idonee e coerenti con il GDPR.

Seppure nel caso specifico sarebbe risultata mancante da parte dell'azienda una regolamentazione interna particolarmente dettagliata in ordine ai limiti nell'uso della casella di posta elettronica (soprattutto con riguardo alle specifiche riguardanti l'attività di backup ed i tempi di conservazione dei dati) – presupposti di compliance organizzativa ormai indispensabili - è pur vero che un esame di "sistema" del **provvedimento** porta a considerarlo nel caso specifico **comunque eccessivo**. Ed è proprio dall'esame delle sue criticità che emergono alcuni **utili spunti di riflessione**.

L'Autorità ribadisce come sia davvero molto sottile la **linea di confine** tra ciò che riguarda l'**ambito lavorativo** e ciò che costituisce "***patrimonio individuale***". Sulla base di tale dato, sarebbe quindi auspicabile per le aziende prevedere sistemi di classificazione e conservazione strutturata di tutta la documentazione e attività aziendale (posta elettronica compresa), invece che fare affidamento solo sui sistemi di individualizzazione delle e-mail. In tal modo si potrebbero realizzare i presupposti per rendere più tracciabile l'uso e la conservazione dei dati (di tutti i dati, compresi i dati aggregati ricavabili dalla posta elettronica) assicurando la tutela del patrimonio informativo aziendale e riducendo i rischi in caso di (legittima) richiesta di accesso da parte dei dipendenti.

Si tratta di questioni che – complice proprio l'evoluzione tecnologica - sono strettamente connesse alla necessità di predisporre **idonee, dettagliate ed efficaci policy interne**. È sempre utile (se non addirittura ormai necessario) implementare regolamenti aziendali che definiscano e comunichino in modo completo ed esaustivo le regole tecniche e le procedure per l'utilizzo degli strumenti informatici, inclusi i limiti sull'uso personale di tutti gli strumenti di lavoro (casella di posta elettronica compresa) affiancandovi una **informativa privacy** che specifichi in modo puntuale:

- finalità e modalità di trattamento;
- base giuridica;
- categoria di dati trattati;
- periodo di conservazione;
- diritti dell'interessato:
- l'esistenza di eventuali processi decisionali automatizzati, così come previsto dalla legge (art. 13 GDPR, art. 1-bis D.Lgs. 152/1997; art. 11 L. 132/2025).

Approccio proattivo alle richieste di accesso

Altro aspetto critico che emerge dalla vicenda è la concreta **prevedibilità della richiesta**: l'accesso ai dati non può più essere gestito come un **evento eccezionale** ma deve, al contrario, essere incardinato in un **flusso procedurale definito**, che consenta all'azienda di rispondere alle richieste in modo adeguato, tempestivo e verificabile.

Occorre **individuare i responsabili** della gestione dell'istanza, i tempi di lavorazione, stabilire criteri oggettivi di estrazione dei dati, nonché prevedere **tecniche standardizzate** di oscuramento o pseudonimizzazione, accompagnate da una motivazione puntuale delle eventuali limitazioni. Ogni fase del processo dovrebbe essere **documentata e tracciata** – anche con l'ausilio del DPO cui sono demandate le più complesse procedure tecniche di assessment- così da poter dimostrare, anche *ex post*, la correttezza delle scelte effettuate (anche alla luce delle numerose e pervasive Linee guida periodicamente emanate dal Garante della privacy).

Conclusioni

In conclusione, il provvedimento segna un punto fermo: la **gestione della e-mail** richiede un approccio strutturato e coerente con i principi di **trasparenza, minimizzazione e *accountability***. La casella di posta aziendale assegnata individualmente si conferma uno spazio ibrido, in cui si intrecciano esigenze organizzative, diritti del lavoratore e interessi dell'impresa, imponendo al datore di lavoro elevati livelli di analisi, di gestione e di compliance. **Non si tratta più di stabilire "*se*" consentire l'accesso, ma "*come*"**: il focus si sposta dalla singola decisione alla solidità del sistema che la sostiene. **La compliance si gioca quindi *ex ante***, nella capacità di progettare sistemi di conservazione, policy e procedure non standardizzate che rendano la casistica delle richieste gestibile e difendibile.

Permangono, tuttavia, **margini di incertezza** che suggeriscono un approccio prudente e documentato alla gestione di questa complessa materia in azienda.

Il messaggio è chiaro, l'e-mail aziendale non è più un semplice strumento tecnico, ma un uno strumento di lavoro che va regolato in modo puntuale. **Dove manca organizzazione aumenta il rischio**, dove c'è metodo si rafforzano compliance ed efficienza, evitando effetti e ricedute negative a carico delle aziende.