LABOR Il lavoro nel diritto

Pacini Giuridica

Privacy e lavoro: registrazioni, investigazioni e controlli tra diritto di difesa e principio di necessità

di F. Pisani - *10 ottobre 2025*

Negli ultimi mesi il dibattito in tema di controlli a distanza si è intensificato, a seguito di importanti decisioni del Garante per la protezione dei dati personali e della Corte di cassazione. Il filo conduttore è la ricerca di un equilibrio tra poteri datoriali, tutela della riservatezza e diritto di difesa, in un contesto segnato dall'uso sempre più pervasivo di strumenti digitali.

Con il provvedimento n. 243 del 29 aprile 2025, il Garante ha sanzionato la Regione Lombardia per un complesso di violazioni in materia di trattamento dei dati dei dipendenti, emerse a seguito di verifiche sull'utilizzo degli strumenti informatici aziendali. L'Autorità ha ritenuto illecito il trattamento dei metadati della posta elettronica e dei log di navigazione internet, effettuato senza la previa stipula di un accordo sindacale o, in alternativa, senza l'autorizzazione dell'Ispettorato nazionale del lavoro, come prescritto dall'art. 4, co. 1, della l. n. 300/1970. In tale condotta sono state ravvisate violazioni degli artt. 5, 6 e 88 GDPR nonché degli artt. 113 e 114 del Codice privacy.

Dall'istruttoria è emerso che la Regione conservava i metadati delle e-mail per 90 giorni e i log di navigazione per 365 giorni. Tali periodi di conservazione, giudicati eccessivi e sproporzionati, sono stati ritenuti idonei a configurare un controllo indiretto e generalizzato sull'attività lavorativa, in contrasto con i principi di liceità, necessità e minimizzazione sanciti dal GDPR. È stato inoltre sottolineato come la possibilità di ricostruire *ex post*, attraverso tali archivi, i comportamenti digitali dei dipendenti costituisca un trattamento invasivo della sfera privata, anche in assenza di un monitoraggio in tempo reale.

Il Garante ha censurato, inoltre, la mancata effettuazione di una valutazione d'impatto (DPIA) ai sensi dell'art. 35 GDPR, nonostante la natura sistematica, estesa e potenzialmente intrusiva del trattamento, nonché le carenze nella regolamentazione dei rapporti con i responsabili del trattamento, che non garantivano un adeguato livello di conformità. La Regione si è così resa inadempiente non solo rispetto ai principi generali di correttezza e trasparenza, ma anche rispetto al principio di responsabilizzazione (art. 5, par. 2, GDPR), che impone al titolare di dimostrare la conformità dei trattamenti.

Per tali violazioni, l'Autorità ha irrogato una sanzione amministrativa di 50.000 euro e ha ingiunto alla Regione di adottare una serie di misure entro 90 giorni. Tra queste: l'anonimizzazione dei tentativi di accesso a siti web bloccati, la riduzione a 90 giorni del periodo massimo di conservazione dei log di navigazione, la cifratura dei nominativi dei dipendenti associati ai dati raccolti, nonché l'adozione di idonee misure organizzative a presidio della riservatezza.

Il provvedimento si inserisce in una linea interpretativa più ampia, che trova conferma anche nel provvedimento n. 288 del 21 maggio 2025, con cui il Garante ha dichiarato illecito il trattamento effettuato da Autostrade per l'Italia S.p.A., che aveva utilizzato contenuti provenienti dai profili Facebook, Messenger e WhatsApp di una dipendente per fondare due contestazioni disciplinari. L'azienda sosteneva la liceità del trattamento richiamando il legittimo interesse e il diritto di difesa.

L'Autorità ha invece rilevato che l'acquisizione e l'utilizzo di tali contenuti integravano un vero e proprio trattamento di dati personali, ai sensi dell'art. 4, n. 2, GDPR, anche se originariamente trasmessi da terzi o ricevuti passivamente. In particolare, i dati in questione riguardavano comunicazioni private destinate a una cerchia ristretta di persone, rientranti nella nozione di corrispondenza protetta dall'art. 15 Cost. e dall'art. 8 CEDU, e non attinenti all'attitudine professionale del lavoratore (art. 113 Codice Privacy; art. 8 Stat. lav.).

Il Garante ha sottolineato come la raccolta e l'uso di tali comunicazioni violino i principi di liceità, correttezza, finalità e minimizzazione (artt. 5, 6 e 88 GDPR), poiché non sorretti da una base giuridica idonea e non proporzionati rispetto allo scopo perseguito. Inoltre, è stato ribadito che la garanzia della riservatezza non viene meno neppure quando il contenuto divenga, di fatto, conoscibile da altri, giacché il datore di lavoro non può trasformare tale circostanza in una fonte di controllo.

In applicazione dei propri poteri, l'Autorità ha inflitto ad Autostrade una sanzione amministrativa pecuniaria (quantificata in relazione alla gravità e alla durata delle violazioni) e ha affermato l'inutilizzabilità dei dati raccolti, anche ai fini disciplinari. Di particolare rilievo è la precisazione secondo cui il diritto di difesa del datore non può prevalere sul principio di necessità, che impone di limitare i trattamenti a quanto strettamente indispensabile e nel rispetto della proporzionalità.

I due provvedimenti, seppur in contesti diversi, tracciano una linea chiara: il datore di lavoro non può esorbitare dai limiti posti dalla disciplina sui controlli a distanza e sulla pertinenza dei dati, né può trasformare segnalazioni spontanee o contenuti di social network in strumenti di sorveglianza indiscriminata. Il principio cardine resta quello della proporzionalità e minimizzazione, a tutela della dignità e della riservatezza del lavoratore, anche nell'era digitale.

Una linea confermata anche dalla Newsletter n. 535 del 30 maggio 2025, nella quale l'Autorità ha chiarito che il controllo su e-mail e navigazione è possibile solo a condizione di un'informativa chiara, di tempi di conservazione ragionevoli e di un previo accordo sindacale o autorizzazione amministrativa.

Ed ancora, con le Newsletter n. 534 dell'8 maggio e 536 del 25 giugno 2025 è stato, rispettivamente, escluso l'uso generalizzato di strumenti di geolocalizzazione nei confronti di dipendenti in *smart working* (ritenuto sproporzionato e non giustificato da una base normativa adeguata) e vietato l'impiego di dati biometrici, come le impronte digitali, per rilevare le presenze (salvo che un'apposita norma di legge non lo consenta in circostanze particolari).

Su questo sfondo si collocano le recenti pronunce della Cassazione, che hanno rafforzato la portata applicativa dei principi indicati dal Garante.

L'ordinanza n. 20487 del 21 luglio 2025 (in corso di pubblicazione in *www.rivistalabor.it*, con nota di P. DUI, *La Cassazione sulla registrazione clandestina tra colleghi: quando non opera la scriminante difensiva*) e l'ordinanza n. 23578 del 20 agosto 2025 (di prossima pubblicazione in www.rivistalabor.it, commentata da P.DUI), insieme alla sentenza n. 24204 del 29 agosto 2025 della Suprema Corte (anche questa di prossima pubblicazione in *www.rivistalabor.it*, commentata da A. CIRACO'), hanno offerto ulteriori chiarimenti sulla liceità delle registrazioni occulte di conversazioni sul luogo di lavoro e sull'utilizzo di agen-

zie investigative per verificare comportamenti sospetti dei dipendenti durante periodi di assenza.

Nel caso affrontato con l'ordinanza di luglio, la Suprema Corte ha ritenuto che la registrazione effettuata dal lavoratore possa essere legittima se finalizzata esclusivamente all'esercizio del diritto di difesa in giudizio, purché rispetti i principi di necessità, proporzionalità e minimizzazione. Non si tratta, dunque, di una facoltà illimitata: l'uso di tali registrazioni deve rimanere confinato allo stretto indispensabile per la tutela dei propri diritti e non può tradursi in una sorveglianza sistematica e permanente della vita lavorativa altrui. La Cassazione ha quindi confermato da validità della sanzione inflitta al dipendente che era stato sospeso proprio per aver clandestinamente registrato una conversazione tra colleghi.

La seconda pronuncia, l'ordinanza n. 23578 del 20 agosto 2025, ruota attorno all'utilizzo di controlli difensivi esterni, affidati a un'agenzia investigativa, per verificare l'effettiva reperibilità di un lavoratore durante un periodo di malattia. In questo caso la Cassazione ha ritenuto illegittima la condotta (stavolta datoriale), poiché la decisione di avvalersi dell'agenzia non era fondata su elementi oggettivi e concreti che giustificassero il ricorso a uno strumento invasivo. La Corte ha sottolineato che il potere di controllo non può trasformarsi in una forma di sorveglianza preventiva e generalizzata: occorrono circostanze specifiche e documentate, tali da integrare un fondato sospetto di irregolarità. Solo in presenza di tali condizioni diventa lecita la raccolta di dati personali attraverso modalità che incidono sulla sfera privata del dipendente.

Infine, con la sentenza n. 24204 del 29 agosto 2025, la Corte ha precisato che il datore di lavoro, in assenza di adeguata informativa, non può accedere alla posta elettronica degli ex dipendenti, anche se gli account sono utilizzati per ragioni lavorative e risiedevano sui server aziendali. Tale principio si fonda sulla tutela della privacy e della corrispondenza privata, che rimangono inviolabili anche dopo la cessazione del rapporto di lavoro. L'accesso non autorizzato costituisce una violazione della normativa sul trattamento dei dati personali e relativa all'accesso abusivo a sistemi informatici. Inoltre, i dati ottenuti in violazione di queste norme risultano inutilizzabili in giudizio, rafforzando la protezione del lavoratore e delimitando strettamente i poteri del datore in materia di controllo post-contrattuale.

Dalle recenti indicazioni della Cassazione e del Garante emerge concretamente l'importanza del principio di necessità e minimizzazione: che si tratti di conversazioni, immagini, metadati di e-mail o log di navigazione, la raccolta e il trattamento dei dati devono essere sempre limitati a quanto strettamente richiesto dalla finalità legittima perseguita e predeterminata, escludendo ogni forma di raccolta preventiva, massiva o sproporzionata, con la conseguenza che, anche in contesti giudiziari, tali principi prevalgono sul diritto di difesa, impedendo al datore o alle parti di acquisire dati oltre i limiti stabiliti dalla legge sulla protezione della *privacy*.

Questi interventi, letti complessivamente, offrono nuove utili indicazioni sulle modalità delle forme di controllo. Si tratta di due approcci che si completano delineando i limiti del diritto di difesa e il rispetto della cornice regolamentare e tecnica prevista dal GDPR e dal Codice privacy.

Per le imprese, il messaggio complessivo è chiaro: la gestione dei controlli sui dipendenti non può essere improvvisata. È necessario predisporre policy interne trasparenti, negoziarle quando richiesto con le rappresentanze sindacali, effettuare valutazioni d'impatto sui trattamenti più invasivi, adottare strumenti di anonimizzazione e limitare i tempi di conservazione dei dati. Allo stesso tempo sarà cruciale formare dirigenti e responsabili delle risorse umane sui principi di proporzionalità, necessità e minimizzazione, così da prevenire contenziosi giudiziari e sanzioni amministrative.

In un contesto in cui l'uso di tecnologie digitali, intelligenza artificiale e sistemi di monitoraggio cresce in maniera esponenziale, il rischio di travalicare i confini della liceità è concreto. Proprio per questo le aziende che sapranno coniugare esigenze organizzative e tutela della privacy non solo ridurranno la propria esposizione al rischio di rivendicazioni a seguito dell'utilizzo improprio di dati raccolti tramite strumenti di controllo, ma rafforzeranno anche il rapporto fiduciario con i propri dipendenti, trasformando la compliance da obbligo difensivo a leva strategica di gestione delle risorse umane.

Federico Pisani, avvocato e consulente del lavoro in Roma e professore a contratto in diritto della sicurezza sociale nell'Università degli Studi di Cassino e del Lazio Meridionale

Visualizza i documenti: Garante privacy 29 aprile 2025, n. 243; Garante privacy 21 maggio 2025, n. 288