AVV. PAOLA IMMERINI
Via Roma 7 – 36040 Grumolo delle Abbadesse (VI)
C.F.MMRPLA74S53L840H – P.IVA03317770240
Recapiti: avv.immerini@libero.it - 349-6802081

Grumolo delle Abbadesse 22 agosto 2025

Provvedimento sanzionatorio del Garante della Privacy n.243 del 29 aprile 2025 nei confronti della Regione Lombardia – utilizzo dei Metadati e della posta elettronica per un controllo indiretto del lavoratore – indicazioni operative utili alle Pubbliche Amministrazioni

Il Garante ha sanzionato, con Provvedimento n.243 del 29 aprile 2025, la Regione Lombardia per aver effettuato il trattamento dei metadati di posta elettronica in violazione degli artt. 5, par. 1, lett. a), 6, 35 e 88 del Regolamento, nonché dell'art.114 del Codice della Privacy; il trattamento dei log di navigazione in Internet in violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 25, 35 e 88 del Regolamento, nonché degli artt.113 e 114 del Codice della Privacy; il trattamento dei dati personali contenuti nel sistema OTRS in violazione degli artt. 5, par. 1, lett. e), 25 e 28 del Regolamento. La sanzione amministrativa applicata è di € 50.000,00.

Nel caso oggetto di sanzione, la Regione Lombardia conservava per 90 giorni i metadati relativi alle email (mittente, destinatario, oggetto, data e ora) dei propri dipendenti.
Il Garante rilevava come:

- La raccolta avvenisse in modo generale e preventivo e non in risposta a situazioni specifiche documentate;
- Non fosse stata adottata alcuna delle misure previste a tutela dei lavoratori (accordo sindacale o autorizzazione dell'INL) prima della raccolta;
- Non fosse stata svolta una valutazione di impatto sulla protezione dei dati personali anche con riferimento al trattamento dei metadati relativi all'utilizzo della posta elettronica;
- Il periodo di conservazione dei dati eccedesse di molto i 21 (ventuno) giorni indicati dal Garante nel precedente provvedimento n.364 del 6 giugno 2024.

Si riassumono, in particolare, gli aspetti salienti del Provvedimento dai quali si evince che:

- I metadati sono parte integrante della gestione tecnica dell'infrastruttura IT e quindi del patrimonio informativo del datore di lavoro.
- Pur non essendo utilizzati "dichiaratamente" per il controllo dei lavoratori, sono tecnicamente idonei a consentirlo, anche attraverso processi di ricongiunzione dei dati e monitoraggi mirati.

1.La posta elettronica può rientrare tra "gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" solo se è funzionale all'attività lavorativa.Tale eccezione prevista dall'art. 4 comma 2, della legge n.300/1970, deve essere interpretata in modo restrittivo e di norma, quindi, rientrano nell'eccezione solo software e applicativi necessari per svolgere le mansioni lavorative. Quando invece gli strumenti, come ad esempio i sistemi di posta elettronica, permettono anche forme di raccolta automatica, non percepibile o generalizzata di dati (come i metadati) o consentono al datore di lavoro di effettuare elaborazioni ulteriori per proprie finalità, si configura un rischio di controllo indiretto sull'attività del dipendente. In questi casi, non è applicabile l'eccezione del comma 2, ma trova applicazione la disciplina ordinaria del comma 1, che prevede specifiche garanzie. Soltanto la raccolta limitata dei metadati strettamente necessari al funzionamento del sistema, per pochi giorni (di norma non oltre 21), può ricadere nell'ambito dell'eccezione, a condizione che siano rispettati il principio di responsabilizzazione e le peculiarità tecnico-organizzative del titolare. In assenza di tali requisiti, è necessario attivare le garanzie del comma 1.

2.Nel caso in esame il trattamento dei metadati di posta elettronica e di navigazione in internet è stato svolto senza una valutazione di impatto preventiva, in violazione dell'art. 35 del Regolamento (GDPR). Spetta al titolare verificare se il trattamento comporti un rischio elevato per metadati e log (ad esempio informazioni

sui destinatari, oggetto delle email o connessioni ai siti web visitati) per periodi lunghi (ad esempio 90 giorni), si configurino trattamenti ad alto rischio. Ciò è particolarmente rilevante nel contesto lavorativo ove i dipendenti sono considerati soggetti vulnerabili. In tali situazioni, l'impiego di tecnologie di monitoraggio continuo comporta un rischio concreto di controllo delle attività lavorative, anche involontario. Simili trattamenti richiedono una valutazione di impatto preventiva e il rispetto di garanzie rafforzate.

In ogni caso,condizione imprescindibile per la stipula del titolo è la previa individuazione di finalità legittime che possono essere ricondotte alla **tutela del patrimonio informativo dell'ente**, in termini di sicurezza informatica (es. prevenzione del data breach) e di garantire la continuità operativa del sistema IT e di gestire disservizi oltre che dare relativo supporto tecnico.

Alla luce di quanto sopra esposto,per evitare che le pubbliche amministrazioni possano essere sanzionate, si forniscono le seguenti indicazioni operative:

1. **In linea generale**, non è consentita la conservazione dei metadati oltre il termine di 21 giorni e va osservato tale termine in conformità a quanto previsto dal Provvedimento del Garante n.364 del 6 giugno 2024. Gli enti devono essere indirizzati a rispettare tale limite, adottando misure affinché anche i propri fornitori di servizi di posta elettronica si conformino a questo principio.
2. **In via eccezionale**, qualora non sia possibile raggiungere un accordo con il fornitore o, comunque, fino a quando ciò non sia realizzabile, previa valutazione caso per caso della sussistenza di una finalità legittima e proporzionata, è necessario stipulare un accordo sindacale o in mancanza richiedere l'autorizzazione dell'INL.

   Tale accordo/autorizzazione deve essere preceduto da:

- una verifica concreta dell'idoneità tecnica dei metadati a permettere, anche tramite processi di correlazione e monitoraggi mirati, un controllo indiretto sull'attività lavorativa;
- una verifica che la finalità di una conservazione superiore sia riconducibile alla protezione del patrimonio informativo nei termini sopra esposti;
- una valutazione d'impatto sulla protezione dei dati (DPIA), finalizzata ad analizzare i potenziali rischi per i diritti e le libertà fondamentali degli interessati derivanti dal conseguente trattamento dei dati In questi casi, deve essere fornita ai lavoratori un'adeguata informativa ai sensi degli articoli 13 e 14 del Regolamento (UE) n. 2016/679 (GDPR).

Avv. Paola Immerini