Il Garante della *privacy* si pronuncia sul trattamento dei metadati dei dipendenti

10/06/2025

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, CONTENZIOSO

Gaspare Roma
Jacopo Piemonte
Adriano Garofalo
Marco Stillo

Con un provvedimento destinato a creare un precedente in materia, in data 29 aprile 2025 il Garante per la Protezione dei Dati Personali ha emesso la sua prima sanzione ai sensi del Regolamento (UE) 2016/679 (*General Data Protection Regulation*, GDPR)[1] per la conservazione illegittima dei c.d. "metadati"[2] delle e-mail dei dipendenti e delle attività di navigazione *web*, applicando per la prima volta le Linee Guida pubblicate nel giugno 2024[3].

Nell'ambito di accertamenti condotti al fine di verificare l'osservanza delle norme in materia di protezione dei dati personali in relazione ai trattamenti posti in essere in ambito lavorativo da parte della Regione Lombardia, il Garante aveva rilevato che quest'ultima aveva conservato i metadati e i *log* di navigazione, rispettivamente, per 90 e 365 giorni, un periodo di tempo ben superiore a quello previsto dalle Linee

[1] GUUE L 119 del 04.05.2016.
[2] Per "metadati" si intendono i log tecnici generati automaticamente dai sistemi di posta elettronica contenenti dati quali, tra gli altri, indirizzi e-mail di mittente e destinatario, orario di invio/ricezione, dimensioni dei messaggi, la presenza di allegati, gli indirizzi IP dei *server* o dei client coinvolti nell'instradamento del messaggio. Non rientra tra i "metadati", invece, il contenuto delle e-mail e degli eventuali allegati.
[3] Disponibili al seguente LINK.

Guida[4]. La Regione Lombardia, inoltre, aveva conservato dei *log* non anonimi relativi ai tentativi di accesso di ciascun dipendente a siti *web* censiti in un'apposita *black list*. Di conseguenza, il Garante aveva avviato un procedimento nei confronti della Regione Lombardia in quanto il trattamento dei dati in questione risultava contrario i) alla disciplina di settore in materia di controlli a distanza in riferimento alla conservazione dei metadati generati dall'attività del personale dipendente relativamente sia all'utilizzo del servizio di posta elettronica che alla navigazione in internet, ii) alle condizioni previste dalla disciplina di settore con riguardo all'utilizzo dei metadati raccolti per altri fini connessi alla gestione del rapporto di lavoro, e iii) ai tempi di conservazione dei *log* relativi alla navigazione in *internet* nonché dei dati relativi alle richieste di assistenza tecnica.

Il Garante ha preliminarmente ricordato che i metadati di posta elettronica sono assistiti da garanzie di segretezza, tutelate anche costituzionalmente[5], intese ad assicurare protezione al nucleo essenziale della dignità della persona e al pieno sviluppo della sua personalità nelle formazioni sociali, di talché, anche nel contesto lavorativo, sussiste una legittima aspettativa di riservatezza in relazione alla corrispondenza e, analogamente, agli elementi ricavabili dai dati esteriori della stessa, che ne definiscono i profili temporali nonché gli aspetti qualitativi e quantitativi anche in ordine ai destinatari e alla frequenza di contatto (che, a loro volta, sono suscettibili di aggregazione, elaborazione e di controllo). Lo Statuto dei Lavoratori[6], inoltre, individua tassativamente le finalità per le quali gli strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati nel contesto lavorativo, stabilendo precise garanzie procedurali.

Sebbene la Regione Lombardia avesse dichiarato che la posta elettronica veniva utilizzata dal personale dipendente per rendere la prestazione lavorativa, nella nozione di "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" ai sensi dello Statuto dei lavoratori possono ricomprendersi solo servizi, *software* o applicativi strettamente funzionali a quest'ultima. Ciò, tuttavia, non si verifica nel caso in cui i metadati di posta elettronica siano raccolti e conservati, in modo preventivo e generalizzato, per un esteso arco temporale dai programmi e servizi informatici per la gestione della posta elettronica. Tali operazioni di trattamento, infatti, sono effettuate, per esigenze proprie del datore di lavoro, automaticamente e indipendentemente dalla percezione e dalla volontà del lavoratore. I metadati in questione, inoltre, rimangono nella disponibilità

[4] Ossia, rispettivamente, 21 e 90 giorni.
[5] Si vedano gli articoli 2 e 15 della Costituzione.
[6] Legge 20 maggio 1970, n. 300, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento, GU n. 131 del 27.05.1970. L'articolo 4 della Legge, intitolato "Impianti audiovisivi e altri strumenti di controllo", ai paragrafi 1-2 dispone: "*... Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.*
In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze...".

esclusiva del datore di lavoro e, per suo conto, del fornitore del servizio, documentando il traffico anche dopo l'eventuale cancellazione del messaggio da parte del lavoratore, il quale, invece, mantiene la disponibilità dei messaggi che, in qualità di mittente o destinatario, scambia all'interno della casella di posta assegnatagli dal datore di lavoro, con il conseguente rischio di un indiretto controllo a distanza dell'attività dei lavoratori.

In un contesto del genere, pertanto, affinché sia ritenuto applicabile il comma 2 dell'articolo 4 dello Statuto dei lavoratori, l'attività di raccolta e conservazione dei soli metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica e il soddisfacimento delle più essenziali garanzie di sicurezza informatica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, può essere effettuata, di norma, per un periodo limitato a pochi giorni, comunque non superiore ai 21, salvo che il titolare comprovi adeguatamente la ricorrenza in concreto di particolari condizioni che ne rendano necessaria l'estensione in ragione delle specificità della propria realtà tecnica e organizzativa. Diversamente, la generalizzata raccolta e la conservazione dei metadati di posta elettronica, per un lasso di tempo più esteso, in presenza di esigenze comunque riconducibili alla sicurezza e alla tutela del patrimonio anche informativo del datore di lavoro, richiede l'esperimento delle garanzie previste dall'articolo 4, comma 1, dello Statuto, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori.

Dando luogo ad un trattamento generalizzato dei dati relativi all'attività e all'utilizzo dei servizi di rete da parte di dipendenti comunque identificabili, inoltre, la raccolta e la conservazione sistematica di tutti i file di *log* generati dall'utilizzo della rete *internet* nell'ambito del rapporto di lavoro, inclusi quelli relativi ai tentativi falliti di accesso ai siti già censiti all'interno di una apposita *black list*, cui è comunque inibito l'accesso dal sistema, comportano, in presenza di un collegamento univoco con il dipendente e con la sua specifica postazione di lavoro, la possibilità di ricostruirne l'attività mediante l'impiego di sistemi tecnologici, di talché, in tali casi, al datore di lavoro è richiesto di assicurare il rispetto delle garanzie procedurali previste dall'articolo 4, comma 1, dello Statuto dei lavoratori, che costituisce condizione di liceità dello stesso trattamento dei dati in questione. Di conseguenza, dato che la Regione Lombardia aveva raccolto e trattato tutti i *log* di navigazione in *internet* del personale dipendente in assenza della previa stipulazione di un accordo collettivo con le competenti parti sindacali, il trattamento in questione è avvenuto, entro i limiti di tale arco temporale, in violazione del GDPR.

Tutto ciò premesso, pertanto, il Garante ha deciso, da un lato, di sanzionare la Regione Lombardia con un'ammenda pari a 50.000 euro e, dall'altro, di ordinarle, tra le altre cose, di limitare la conservazione dei registri di navigazione a 90 giorni e successivamente procedere all'anonimizzazione, di ridurre al minimo e crittografare i metadati delle e-mail, di limitare l'accesso ai metadati al solo personale autorizzato e di aggiornare le politiche interne e la documentazione sulla *privacy*.

Alla luce di quanto accertato dal Garante, le aziende sono chiamate a rivedere con estrema attenzione le proprie pratiche di gestione dei metadati e dei *log* di rete. Già prima del provvedimento era richiesto un elevato livello di cautela nel trattamento delle e-mail, imponendo, ad esempio, la trasparenza sui controlli effettuati e la cancellazione tempestiva delle caselle dei dipendenti cessati. La recente sanzione introduce un ulteriore livello di attenzione, estendendo l'obbligo di conformità anche ai cosiddetti dati "esteriori", come metadati e *file* di *log,* suscettibili di determinare un controllo indiretto dell'attività lavorativa. A riguardo si nota che i metadati delle *e-mail* dovrebbero essere conservati, di norma, non oltre i 21 giorni, mentre i *log* di navigazione vanno limitati a 90 giorni, seguiti da anonimizzazione. È inoltre fondamentale aggiornare le informative *privacy*, limitare l'accesso ai dati, crittografarli e adottare *policy* interne

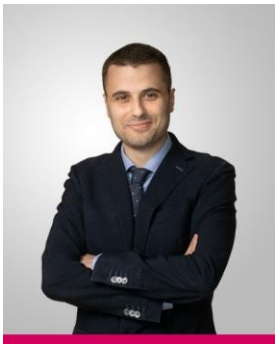
coerenti. Solo un approccio strutturato e rispettoso delle normative potrà garantire la tutela dei diritti dei lavoratori e la conformità aziendale ed evitare conseguenze rilevanti per l'organizzazione, anche sotto il profilo sanzionatorio da parte delle Autorità competenti, come dimostrato dal caso concreto.

Gaspare Roma
PARTNER

g.roma@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Jacopo Piemonte
ASSOCIATE

j.piemonte@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 – Milano
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles



Adriano Garofalo
ASSOCIATE

a.garofalo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Marco Stillo
ASSOCIATE

m.stillo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com