

Nelle email vanno eliminati i dati automatici dei server

Lavoro e privacy

Possono essere conservate le informazioni legate al singolo messaggio

Spetta alle aziende verificare che i programmi rispettino le regole

Giulio Coraggio
Giampiero Falasca

Le nuove linee guida sulla conservazione dei metadati delle email aziendali, approvate dal Garante privacy il 6 giugno (si veda il «Sole 24 Ore» di sabato 15 giugno), contengono delle precisazioni molto importanti per le aziende.

In particolare, le nuove linee guida offrono una definizione molto più precisa, rispetto alle precedenti del 6 febbraio che avevano suscitato tanti allarmi nelle imprese, di cosa si debba intendere per metadati.

Mentre il precedente provvedimento dedicava a questo aspetto poche parole, limitandosi a includere nella nozione alcune informazioni (data, ora, destinatario, oggetto) collegate alle email aziendali, nel nuovo provvedimento si fissa un perimetro più chiaro (e ristretto).

Secondo la nuova disciplina, vanno considerati come metadati le «informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (mail transport agent) e dalle postazioni client (mail user agent)».

In questo modo, il Garante include nella nozione di metadati solo le informazioni tecniche che vengono inserite in modo automatico nei registri (log) indipendentemente dalla volontà dell'utente, e la loro conservazione – secondo il Garante – non può superare i 21 giorni. Queste informazioni consentono al datore di lavoro la consultazione della corrispondenza in entrata accedendo alle caselle di posta elettronica e possono comprendere gli indirizzi email di mittente e destinatario, gli indirizzi IP dei server o client coinvolti, gli orari di invio, ritrasmissione o ricezione, le dimensioni del messaggio, la presenza e dimensione di eventuali allegati e, a volte, l'oggetto del messaggio.

Se le aziende intendono superare il termine di 21 giorni, è necessario l'adempimento degli obblighi previsti dalla normativa privacy (per esempio informativa privacy, data protection impact assessment-Dpia e legittimate interest assessment-Lia), oltre alla stipula di un accordo sindacale oppure l'ottenimento di un'autorizzazione amministrativa, secondo quanto previsto dall'articolo 4 dello Statuto dei lavoratori e ciò può avvenire solo in presenza di «particolari condizioni».

Però questi metadati – e qui c'è l'elemento di novità delle linee guida – sono distinti dalle informazioni che formano il cosiddetto envelope, ovvero l'insieme delle intestazioni tecniche strutturate che documentano l'instradamento del messaggio, la sua provenienza e altri parametri.

Queste ultime informazioni, pur coincidendo con i metadati registrati automaticamente nei log dei servizi di posta, «sono inscindibili dal messaggio di cui fanno parte integrante e

che rimane sotto l'esclusivo controllo dell'utente» e, come tali, non sono soggette al limite di 21 giorni.

Una lettura che cerca di tenere insieme esigenze contrapposte: da un lato, la necessità di limitare il tempo di conservazioni di informazioni che possono generare un controllo a distanza e, dall'altro lato, l'esigenza di legittimare l'involontaria detenzione di informazioni che transitano sui server come parte integrante delle email e rimangono sotto il controllo esclusivo dell'utente.

Bisognerà valutare se, in caso di contenziosi, in concreto i Tribunali considereranno sufficienti a livello probatorio le informazioni che rimangono nell'inbox dei dipendenti che, in mancanza dei log generati dal Mta, potrebbero non essere autentiche e quindi rischiano di essere contestate. Se così non fosse, il nuovo provvedimento del Garante non risolverebbe il problema che rimarrebbe quello che ha suscitato tante lamentele negli ultimi mesi.

Il provvedimento evidenzia, infine, che i software che le aziende usano per gestire le email spesso hanno impostazioni predefinite che potrebbero non essere in linea con la normativa italiana.

Il Garante ricorda alle aziende che è loro responsabilità verificare queste impostazioni e, se necessario, chiedere ai fornitori di modificarle. Le aziende dovranno, quindi, eseguire una dettagliata analisi per comprendere la tipologia di metadati che raccolgono e il tempo di cui necessitano per conservarli. Solo dopo aver fatto questa analisi, potranno valutare quali adempimenti privacy e giuslavoristici sono necessari.