

Approfondimento Rapporti di lavoro

Privacy e posta elettronica, alleggerimento degli oneri

di Luca Failla e Paola Salazar

N. 26 - 25 Giugno 2024

I. Guida al Lavoro

Le linee guida del Garante sulla conservazione dei metadati dei sistemi di posta elettronica

A dicembre 2023 il Garante Privacy aveva pubblicato un atto di indirizzo sulla conservazione dei metadati della posta elettronica - Provvedimento 21 dicembre 2023, n. 642 intitolato *“Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati* - con l’obiettivo di promuovere una più attenta consapevolezza dei rischi derivanti dall’adozione da parte dei titolari del trattamento di scelte tecniche e organizzative che in qualità di datori di lavoro potessero avere come conseguenza una minor tutela dei lavoratori, sia dal punto di vista degli obiettivi di protezione dei dati, sia dal punto di vista – più specifico – di tutela della libertà e dignità degli stessi scaturente dalle disposizioni dello Statuto dei lavoratori (artt. 4 e 8 L. n. 300/1970). In particolare, con riferimento alle previsioni relative al rischio di controllo a distanza e quindi, alla violazione delle disposizioni dell’art. 4 dello Statuto per forme di controllo occulto.

Il provvedimento di dicembre aveva suscitato da subito alcune critiche e ragionevoli perplessità in ragione del rischio davvero concreto di complicare enormemente la gestione dell’impresa con un ulteriore adempimento di natura tecnica (e amministrativa) che seppure legittimo nel quadro degli obiettivi del GDPR (Reg. UE n. 679/2016) quindi sia in termini di *“responsabilizzazione”* del titolare e di *“valutazione d’impatto sulla protezione dei dati”* connessi agli strumenti ITC, avrebbe potuto creare non poche difficoltà pratiche in termini di organizzazione dell’attività dell’impresa.

Proprio con la consapevolezza delle difficoltà generate da tale provvedimento, il Garante Privacy, aveva poi deciso di avviare – con provvedimento del 22 febbraio 2024 - una consultazione pubblica sul provvedimento, invitando tutti i soggetti interessati ad inviare al Garante le proprie osservazioni, i commenti, le informazioni, le proposte e tutti gli elementi ritenuti utili per poter definire i limiti di congruità del provvedimento e dei suoi obiettivi – soprattutto con riferimento al termine di conservazione dei metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica - rispetto alle finalità perseguite dai datori di lavoro pubblici e privati. Nelle more delle consultazioni era stata pertanto differita l’efficacia del documento fino al completamento delle stesse.

Il nuovo provvedimento del Garante Privacy

Con provvedimento del 6 giugno scorso, a conclusione delle consultazioni, il Garante è quindi tornato sul precedente provvedimento di dicembre adottandone una versione aggiornata. Il nuovo provvedimento -sempre denominato Documento di indirizzo - spicca subito per due rilevanti novità:

a) una più precisa indicazione di cosa si intende per “metadati” ossia solo quelli registrati automaticamente dai sistemi di posta elettronica: *“tecnicamente le informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell’interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l’invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent)”*.

b) il carattere meno precettivo del provvedimento che, proprio perché è comunque un Documento di indirizzo non può – si legge nell’Introduzione - *“recare prescrizioni, né introduce nuovi adempimenti a carico dei titolari del trattamento ma intende offrire una ricostruzione sistematica delle disposizioni applicabili (...) al solo fine di richiamare l’attenzione su alcuni punti di intersezione tra la disciplina di protezione dei dati e le norme che stabiliscono le condizioni per l’impiego degli strumenti tecnologici nei luoghi di lavoro”*.

I metadati: definizione

Con riguardo al primo aspetto il Garante precisa che i metadati cui si riferisce l'Atto di indirizzo non vanno confusi con le informazioni contenute nei messaggi di posta elettronica (nella loro body-part, ossia il corpo del messaggio) o anche in essi integrate a formare quello che tecnicamente viene definito *"envelope"* ossia l'insieme delle intestazioni tecniche strutturate che documentano l'instradamento del messaggio, la sua provenienza e gli altri parametri tecnici, inscindibili dal messaggio e che *"restano sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi)"*.

Raccolta e conservazione dei metadati

Con riguardo al secondo aspetto, nell'Introduzione del documento il Garante precisa che *"stante la natura orientativa del documento di indirizzo, dallo stesso non discendono nuovi adempimenti e responsabilità"*.

Si tratta di aspetti di primaria importanza che mettono in evidenza la logica non più *"prescrittiva"* con cui il Documento è stato adottato, utili per poter valutare come tali Linee Guida, nella loro nuova versione potranno influire sulla gestione pratica degli adempimenti e sulle policy privacy e ICT all'interno delle organizzazioni. Va infatti ricordato che la prima versione del Documento di indirizzo, scaturito da alcuni accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo, dai quali sarebbe emerso il rischio di una raccolta indifferenziata e generalizzata dei *"metadati"* da parte dei programmi e i servizi informatici per la gestione dei sistemi di posta elettronica, presentava una chiara impostazione sia precettiva che sanzionatoria, in termini di possibile violazione della disciplina di riferimento in materia di divieto di controllo a distanza. Tali presupposti avevano portato il Garante a stabilire che ai fini della conservazione dei dati (tecnici) collegati con i programmi e i servizi informatici per la gestione della posta elettronica dovessero trovare applicazione le garanzie procedurali e amministrative previste delle disposizioni dell'art. 4 L. n. 300/1970.

E ciò sul presupposto – oggi molto ridimensionato – che l'attività di raccolta e conservazione dei soli c.d. metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica *"non potesse essere superiore di norma a poche ore o ad alcuni giorni, in ogni caso non oltre sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustificassero il prolungamento, di ulteriori 48 ore"*.

Diversamente, la generalizzata raccolta e la conservazione di tali metadati – ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro – avrebbe potuto comportare il rischio di un indiretto controllo a distanza dell'attività dei lavoratori, richiedendo l'esperimento delle garanzie previste dall'art. 4, comma 1, L. n. 300/1970, con la conseguenza di dover sottoporre l'uso dei programmi informatici deputati alla gestione – e conservazione – della posta elettronica, alla procedura di accordo sindacale e/o di autorizzazione amministrativa espressamente previsti dalla citata disposizione.

Oggi nella nuova versione del Documento tali criteri risultano molto ridimensionati, innanzitutto in termini temporali – si ritiene che a titolo orientativo, tale conservazione non debba comunque superare i 21 giorni – e poi, significativamente in termini di presupposti oggettivi, poiché si tiene conto da un lato del fatto che possano esserci esigenze di conservazione dei dati (ma intesi come body-part o corpo del messaggio) e dall'altro che l'insieme delle intestazioni e dei parametri tecnici che fanno normalmente parte dell'envelope nel suo complesso, quando legati agli altri elementi che accompagnano il messaggio (quali oggetto, mittente, destinatario, data, ora, frequenza di contatto e così via) seppure possano determinare il rischio di acquisizione di dati riferibili alla sfera personale e alle opinioni dell'interessato – tutelati dall'art. 8 e dall'art. 4 L. n. 300/1970 – possano e debbano essere comunque gestiti sulla base dei principi del GDPR.

Quegli stessi principi che governano solitamente (o dovrebbero governare) la procedure interne sulla gestione e l'utilizzo degli strumenti di lavoro: dalla scelta delle applicazioni, dei servizi, dei prodotti, alla scelta di fornitori che possano assicurare al titolare del trattamento l'assolvimento degli obblighi che scaturiscono dal GDPR nel rispetto dei principi stabiliti dall'art. 4 Statuto dei Lavoratori e, soprattutto, dell'eccezione prevista dal comma 2 della norma, proprio con riferimento agli strumenti di lavoro e alle informazioni da essi raccolte che, proprio perché essenziali per l'esecuzione della prestazione, se correttamente gestiti, non determinano forme di controllo occulto.

In ragione di ciò, nel richiamare i principi guida rilevanti in questa materia quali: i) liceità del trattamento (che deriva anche dal sottostante rapporto contrattuale ex art. 6 Reg. n. 679/2016); ii) correttezza e trasparenza (art. 5, par. 1 lett. a); 12, 13 e 14 reg. n. 676/2016); iii) limitazione della conservazione (art. 5, par. 1 lett. e); iv) protezione dei dati fin dalla fase di progettazione (privacy by design) e per impostazione predefinita (privacy by default) (art. 5,

par. 2, artt. 24 e 25 Reg n. 679/2016, nonché v) quello di responsabilizzazione del Titolare – soprattutto quando utilizza prodotti e servizi realizzati da terzi in modalità cloud o as-a-service - il Documento finisce per ribadire come risultino essenziali, per le finalità di protezione evidenziate, il rispetto dell'Informativa da rilasciare al lavoratore e, soprattutto, la completezza della stessa anche con riferimento agli obiettivi di conservazione di tali dati.

Non dimentichiamo, infatti, che la posta elettronica – e i relativi programmi informatici di immediato funzionamento – è innanzitutto uno strumento di lavoro e che in quanto strumento di lavoro per espressa scelta del legislatore della riforma (il Jobs Act) – come ricordato anche dal Garante - è in generale sottratto, ai sensi dell'art. 4, c. 2 della L. n. 300/1970 alla procedura e alle garanzie specifiche previste in materia di divieto di controllo a distanza dell'attività lavorativa previsto dallo Statuto dei Lavoratori. E ciò per due fondamentali ragioni. La prima è che la pervasività della tecnologia nella vita quotidiana e nella gestione dell'attività d'impresa deve tutelare la posizione dei lavoratori e le garanzie fondamentali previste dalla legge in materia di divieto di controllo a distanza, ma non deve complicare e burocratizzare in modo eccessivo l'attività delle imprese. Da cui deriva la seconda ragione, ossia che non va mai dimenticata la fondamentale distinzione operata dal legislatore della riforma tra ciò che costituisce "*strumento di lavoro*" sottratto alla procedura autorizzativa (tra cui sono presenti le dotazioni mobili caratterizzate dal PC in uso al dipendente con tutti i programmi in esso installati per le finalità di lavoro) e ciò che non è "*strumento di lavoro*" non essendo "*dotazione*" essenziale per lo svolgimento dell'attività lavorativa (come ad esempio le videocamere che rispondono ad altre finalità) il quale richiede il fondamentale rispetto dei principi e dei divieti posti dall'art. 4 L. n. 300/1970, quale fondamentale espressione di un'esigenza di bilanciamento tra la necessità di conformarsi alla moderna organizzazione d'impresa – considerato l'uso e la pervasività della tecnologia nel normale svolgimento della prestazione lavorativa - e la necessità del rispetto di alcuni principi fondamentali di tutela dei dati, della riservatezza e della dignità morale del lavoratore tutelati dagli artt. 4 e 8 della L. n. 300/1970 (cfr. sul punto la nota Min. Lav. 18 giugno 2015).

La posta elettronica aziendale è ormai divenuta uno strumento di gestione dell'impresa, di gestione dei rapporti contrattuali con clienti e fornitori e certamente - come molte aziende molto opportunamente specificano pure nelle policies di gestione degli strumenti informatici - non viene, né può essere utilizzata per fini personali. La conservazione dei dati – anche dei metadati nell'accezione più precisa fornita dal Garante - che identificano quel documento e che lo rendono rilevante (e legittimo ai sensi dell'art. 6 Reg. UE n. 679/2016) per la gestione da parte del Titolare del trattamento delle proprie relazioni contrattuali - essenziali per lo svolgimento dell'attività d'impresa - deve poter avvenire per tutto il tempo necessario alla gestione degli obblighi che scaturiscono – o che possono scaturire – da quelle informazioni. Per tali ragioni e per l'importanza degli obblighi che derivano dalla conservazione o meno di tali dati, non è possibile prevedere in capo al Titolare obblighi amministrativi analoghi a quelli previsti per l'installazione dei sistemi di video-sorveglianza, ma il rispetto degli adempimenti necessari per la corretta gestione degli strumenti di lavoro quali l'obbligo - in fase di assunzione e ogniquale volta si renda necessario sulla base dell'evoluzione tecnologica – della consegna al lavoratore di una informativa completa e dettagliata ex art. 13 del Reg. UE n. 679/2016 anche con riferimento all'uso di tutte le dotazioni hardware e software, ivi compresi i sistemi di gestione della posta elettronica che, come tutti i lavoratori già sanno, viene concessa e utilizzata unicamente come strumento di lavoro e non personale.

Regola che è nella maggior parte dei casi chiaramente specificata dalle policies aziendali in materia. Da qui la necessità di poter agevolmente conservare i dati, quando necessario, anche oltre il limite – puramente orientativo – individuato oggi dal Garante (21 giorni) se tutti i richiamati principi di liceità, trasparenza e responsabilizzazione sono comunque rispettati dal Titolare, anche sotto il profilo della scelta dei fornitori dei prodotti e servizi. Da un punto di vista pratico, pertanto, oltre all'attenzione nella scelta dei fornitori e alla revisione delle Informative ex art. 13 GDPR – che non devono mai essere considerati documenti statici da rilasciare solo in fase di assunzione al contrario dovendoli sottoporre a revisione e aggiornamento periodici (oggi peraltro richiesto incessantemente dalla tecnologia) - potrebbe essere altresì utile prevedere policies aziendali più stringenti e rigorose nelle quali venga comunque espressamente ribadito il divieto da parte dei lavoratori – sancito anche eventualmente anche con il richiamo alle sanzioni disciplinari contrattualmente previste – sull'uso della casella di posta elettronica per motivazioni private, ribadendo ulteriormente che l'utilizzo della posta elettronica è previsto unicamente per motivi di lavoro e per finalità allo stesso connesse.

Il Sole 24 ORE aderisce a  **The Trust Project**

P.I. 00777910159 © Copyright Il Sole 24 Ore Tutti i diritti riservati

