LE LINEE GUIDA AGGIORNATE SULLA POSTA ELETTRONICA E LA PRIVACY

Nuovo documento di indirizzo Garante privacy n.364 del 6.6.2024 sulla gestione delle mail dipendenti e dei metadati nel contesto lavorativo.

Quaderni Tecnici

Posta elettronica dipendenti e Privacy: linee guida aggiornate 2024

Nuovo documento di indirizzo Garante privacy n.364 del 6.6.2024 sulla gestione delle mail dipendenti e dei metadati nel contesto lavorativo. Ridimensionato l'impatto

Con provvedimento n. 364 del 6 giugno 2024, del Garante per la privacy sono state pubblicate le nuove linee guida in tema di **protezione dei dati personali nella gestione della posta elettronica dei dipendenti**. Si tratta in particolare del Documento di indirizzo "*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*"

Nel Documento viene illustrata la normativa vigente con particolare riguardo alle possibili responsabilità per i **datori di lavoro pubblici e privati**.

Da segnalare una importante novità rispetto al recente documento del 6 febbraio 2024 sullo stesso tema che aveva creato molto allarme tra i datori di lavoro a causa delle forti restrizioni temporali sulla gestione delle mail dei dipendenti.

> *In particolare nelle nuove linee guida che sostituiscono le precedenti, viene chiarito che per metadati si intendono le informazioni generate automaticamente dai server di gestione della posta elettronica aziendale riguardanti invii, ricezione e smistamento e che possono comprendere gli indirizzi email del mittente e del destinatario, indirizzi IP, orari di invio, di trasmissione o di ricezione, dimensioni e presenza di allegati.*

Sono questi dati e non il contenuto nel corpo delle mail né la cosiddetta" *envelope*" che vanno eliminati con le scadenze molto restrittive (al massimo 21 giorni di archiviazione) indicate dal provvedimento del 6 febbraio.

Il chiarimento ridimensiona fortemente l'impatto sulla gestione aziendale trovando un punto accettabile di equilibrio tra protezione dei dati personali ed esigenze organizzative.

Nelle linee guida del 6 febbraio 2024 si analizzava l'utilizzo di programmi forniti in *modalità cloud* che spesso trattano in modo generalizzato e sistematico i dati senza possibilità di disabilitare o modificare le modalità di archiviazione, con possibile violazione delle norme vigenti.

Nel provvedimento il Garante chiedeva quindi ai datori di lavoro di verificare che i programmi e i servizi informatici di gestione della posta elettronica in uso ai dipendenti consentano di modificare

le impostazioni di base, impedendo la raccolta dei metadati o limitando il loro periodo di conservazione

Il periodo considerato congruo sotto il profilo prettamente tecnico, per assicurare il regolare funzionamento della posta elettronica del lavoratore era fissato a un massimo di 7 giorni, estensibili, in presenza di comprovate esigenze, di ulteriori 48 ore.

Per i casi in cui i datori di lavoro debbano per esigenze organizzative e produttive o di tutela del patrimonio informativo del titolare (ad esempio, per specifiche esigenze di sicurezza dei sistemi) trattare i metadati per un periodo di tempo più esteso, si richiede adempiere agli obblighi previsti dalla normativa privacy (per esempio informativa privacy, data protection impact assessment-Dpia e legitimate interest assessment-Lia), e di espletare le procedure di garanzia previste dallo Statuto dei lavoratori (Legge 300 1970) ovvero

- pervenire ad un accordo con le rappresentanze sindacali oppure
- ottenere l'autorizzazione dell'ispettorato del lavoro.

Si allegano:

- Provvedimento n. 364 del 6 giugno 2024

- Documento del 6 febbraio 2024

Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati [10026277]

[doc. web n. 10026277]

Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati

Registro dei provvedimenti
n. 364 del 6 giugno 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, “Regolamento generale sulla protezione dei dati” (di seguito, “Regolamento”), con particolare riguardo agli artt. 5, 6 e 88 dello stesso;

VISTO il d.lgs. 30 giugno 2003, n. 196 recante “Codice in materia di protezione dei dati personali”, recante disposizioni per l’adeguamento dell’ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito, “Codice”), con particolare riguardo agli artt. 113 e 114 dello stesso;

VISTI gli artt. 4 e 8 della l. 20 maggio 1970, n. 300, nonché l’art. 10 del d.lgs. 10 settembre 2003, n. 276, fatti salvi dagli artt. 113 e 114 del Codice;

CONSIDERATO che nell’ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica, commercializzati da fornitori in modalità cloud, possano raccogliere, per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all’utilizzo degli account di posta elettronica in uso ai dipendenti, conservando gli stessi per un esteso arco temporale; ciò talvolta ponendo, altresì, limitazioni al cliente (datore di lavoro) in ordine alla possibilità di modificare le impostazioni di base del programma informatico al fine di disabilitare la raccolta sistematica di tali dati o di ridurre il periodo di conservazione degli stessi;

CONSIDERATO che, nel quadro dei compiti attribuiti al Garante volti a promuovere la consapevolezza e la comprensione del pubblico, dei titolari e dei responsabili del trattamento

riguardo a norme, obblighi, rischi, garanzie e diritti stabiliti dal Regolamento anche mediante documenti di indirizzo (art. 57, par. 1, lett. b) e d), del Regolamento art. 154-bis, comma 1, lett. a), del Codice), questa Autorità ha adottato in via preliminare il documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" (provv. del 21 dicembre 2023, n. 642, doc. web n. 9978728) allo scopo di richiamare l'attenzione su taluni 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;

VISTO il provv. del 22 febbraio 2024, n. 127, doc. web n. 9987885, con il quale, considerate le richieste di chiarimenti pervenute al Garante, è stata avviata una consultazione pubblica in merito alla congruità, in relazione alle finalità perseguite dai datori di lavori pubblici e privati, del termine di conservazione dei metadati (di seguito, anche "log") generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica, sospendendo l'efficacia del predetto documento di indirizzo (v. avviso pubblico di avvio della consultazione sul termine di conservazione dei metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica, pubblicato sulla Gazzetta Ufficiale n. 64 del 16 marzo 2024);

VISTE le osservazioni e le proposte pervenute al Garante nell'ambito della predetta consultazione pubblica;

RITENUTO di apportare specifiche modifiche e integrazioni al predetto documento di indirizzo, nella prospettiva di agevolare, altresì, la comprensione dell'ambito dei trattamenti presi in considerazione e delle indicazioni fornite al fine di promuovere la consapevolezza delle scelte tecniche e organizzative dei datori di lavoro, in qualità di titolari del trattamento, nonché di prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la libertà e la dignità dei lavoratori;

RITENUTO, inoltre, di fornire indicazioni anche in merito ai criteri che possano orientare le scelte dei datori di lavoro nell'individuazione dell'eventuale periodo di conservazione dei predetti log, ai fini dell'applicazione dell'eccezione contenuta nell'art. 4, comma 2, della l. 20 maggio 1970, n. 300 rispetto alla regola di cui al comma 1, per assicurare il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica;

RITENUTO, pertanto, di dover adottare una versione aggiornata del Documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" (all. n. 1), che forma parte integrante del presente provvedimento;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

RELATORE il dott. Agostino Ghiglia;

DELIBERA

di adottare una versione aggiornata del Documento di indirizzo denominato *"Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"* (all. n. 1), che forma parte integrante del presente provvedimento.

Roma, 6 giugno 2024

IL PRESIDENTE

Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei

_____

DOCUMENTO DI INDIRIZZO

Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati

1. Introduzione

Nell'ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica, anche qualora commercializzati da fornitori in modalità cloud, possano raccogliere per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti, conservando gli stessi per un esteso arco temporale. Nel seguito del documento si farà riferimento alternativamente ai "metadati di posta elettronica" o "log di posta elettronica".

I metadati cui fa riferimento il presente documento di indirizzo, sottoposto a consultazione pubblica, corrispondono tecnicamente alle 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).

Tali informazioni relative alle operazioni di invio e ricezione e smistamento dei messaggi possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in relazione al sistema di gestione del servizio di posta elettronica utilizzato, anche l'oggetto del messaggio spedito o ricevuto.

I metadati cui ci si riferisce nel presente documento (sia quelli di origine prettamente tecnica sia quelli, come il campo "Oggetto", determinati dagli utenti) presentano la caratteristica di essere registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla percezione e dalla volontà dell'utilizzatore.

Gli stessi metadati come qui intesi non vanno in alcun modo confusi con le informazioni contenute nei messaggi di posta elettronica nella loro "body-part" (corpo del messaggio) o anche in essi integrate - ancorché talvolta non immediatamente visibili agli utenti dei software "client" di posta elettronica (i cosiddetti MUA - Mail User Agent) - a formare il cosiddetto envelope, ovvero l'insieme delle intestazioni tecniche strutturate che documentano l'instradamento del messaggio, la sua provenienza e altri parametri tecnici. Le informazioni contenute nell'envelope, ancorché corrispondenti a 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 (sia esso il mittente o il destinatario dei messaggi).

Pertanto, le indicazioni contenute nel documento relativamente ai tempi di conservazione dei metadati come sopra definiti non riguardano i contenuti dei messaggi di posta elettronica (né le informazioni tecniche che ne fanno comunque parte integrante) che rimangono nella disponibilità dell'utente/lavoratore, all'interno della casella di posta elettronica attribuitagli.

Il presente documento non reca prescrizioni né introduce nuovi adempimenti a carico dei titolari del trattamento ma intende offrire una ricostruzione sistematica delle disposizioni applicabili in tale specifico ambito, alla luce di talune precedenti decisioni dell'Autorità, 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.

In questa prospettiva l'Autorità intende altresì fornire ai datori di lavoro indicazioni in ordine alla possibilità di trattare tali informazioni per consentire il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica, senza necessità di attivare la procedura di garanzia prevista dall'art. 4, comma 1, l. 20/5/1970, n. 300, espressamente richiamata dall'art. 114 del Codice.

Stante la natura orientativa del documento di indirizzo, dallo stesso non discendono nuovi adempimenti o responsabilità.

Alla luce delle osservazioni e delle proposte pervenute al Garante nell'ambito della consultazione pubblica cui il presente documento è stato sottoposto (provv. del 22 febbraio 2024, n. 127, doc. web n. 9987885; Gazzetta Ufficiale n. 64 del 16 marzo 2024), sono state apportate alcune modifiche e integrazioni al presente documento di indirizzo anche con riferimento ai criteri che possano orientare le scelte dei datori di lavoro nell'individuazione dell'eventuale periodo di conservazione dei predetti log, ai fini dell'applicazione dell'eccezione contenuta nell'art. 4, comma 2, della l. 20 maggio 1970, n. 300 rispetto alla regola di cui al comma 1, per assicurare il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica. Sono stati, inoltre, forniti chiarimenti in merito all'ambito oggettivo di applicazione del documento, anche indicando la definizione di metadato, e alla natura del documento. Infine, è stata richiamata l'attenzione dei fornitori dei servizi di posta elettronica sulla necessità di tenere in considerazione del diritto alla protezione dei dati conformemente allo stato dell'arte, già in fase di progettazione di servizi e prodotti.

2. La normativa in materia di protezione dei dati personali

Come costantemente affermato dal Garante, il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.), che proteggono il nucleo essenziale della dignità della persona e il pieno sviluppo della sua personalità nelle formazioni sociali. Ciò comporta che, anche nel contesto lavorativo pubblico e privato, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza (v. punto 5.2 lett. b), delle "Linee guida del Garante per posta elettronica e Internet" del 1° marzo 2007, n. 13, doc. web n. 1387522; cfr., tra i tanti, provv. 4 dicembre 2019, n. 216, doc. web n. 9215890 e i precedenti in esso citati).

Considerato che l'impiego dei predetti programmi e servizi informatici dà luogo a "trattamenti" di dati personali, riferiti a "interessati", identificati o identificabili (art. 4, par. 1, nn. 1) e 2), del Regolamento) nel contesto lavorativo, è necessario che il datore di lavoro, in quanto titolare del trattamento, verifichi la sussistenza di un idoneo presupposto di liceità (cfr. artt. 5, par. 1, lett. a), e 6 del Regolamento) prima di effettuare trattamenti di dati personali dei lavoratori attraverso tali programmi e servizi, rispettando le condizioni per il lecito impiego di strumenti tecnologici nel contesto lavorativo (art. 88, par. 2, del Regolamento).

In particolare, dovrà quindi essere sempre verificata la sussistenza dei presupposti di liceità stabiliti dall'art. 4 della l. 20 maggio 1970, n. 300, cui fa rinvio l'art. 114 del Codice, nonché il rispetto delle diposizioni che vietano al datore di lavoro di acquisire e comunque trattare informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o comunque afferenti alla sua sfera privata (art. 8 della l. 20 maggio 1970, n. 300 e art. 10 d.lgs. 10 settembre 2003, n. 276, cui fa rinvio l'art. 113 del Codice). Gli artt. 113 e 114 del Codice sono infatti considerati, nell'ordinamento italiano, disposizioni più specifiche e di maggiore garanzia di cui all'art. 88 del Regolamento, la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione determina, oltre all'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, par. 5, lett. d) del Regolamento, anche il possibile insorgere di responsabilità sul piano penale (cfr. art. 171 del Codice).

Il titolare del trattamento è inoltre tenuto a rispettare i principi generali del trattamento (artt. 5, 24 e 25 del Regolamento) e a porre in essere tutti gli adempimenti previsti dalle disposizioni normative in materia di protezione dei dati personali (v. artt. 12, 13, 14, 30, 32 e 35 del Regolamento), anche con riguardo alla necessità di fornire agli interessati in modo corretto e trasparente una chiara rappresentazione del complessivo trattamento effettuato, consentendo agli stessi di disporre di tutti gli elementi informativi essenziali previsti dal Regolamento e di essere pienamente consapevole, prima che il trattamento abbia inizio, delle caratteristiche dello stesso (cfr. sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. par. n. 133 e 140).

Inoltre, in attuazione del principio di "responsabilizzazione" (cfr. art. 5, par. 2, e 24 del Regolamento), spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche - in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite - che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali (cfr. cons. 90 e artt. 35 e 36 del Regolamento).

Anche tenuto conto delle indicazioni fornite anche a livello europeo sul punto, tale necessità ricorre, in particolare, in caso di raccolta e memorizzazione dei log della posta elettronica, stante la particolare "vulnerabilità" degli interessati nel contesto lavorativo, nonché il rischio di "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti" (Gruppo di lavoro art. 29, "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento", WP 248 del 4 aprile 2017; cfr. cons. 75 e artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1; v., tra gli altri, provv. 13 maggio 2021, n. 190, doc. web n. 9669974, par. 3.5).

3. La disciplina di settore in materia di controlli a distanza

L'art. 4, comma 1, l. 20 maggio 1970, n. 300, come modificato dal d.lgs. 14 settembre 2015, n. 151, individua tassativamente le finalità (ovvero quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) 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 (accordo sindacale o autorizzazione pubblica).

Le predette garanzie non trovano invece applicazione "agli strumenti di registrazione degli accessi e delle presenze", così come "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970). Tale disposizione introduce un'eccezione, rispetto al più restrittivo regime previsto dal comma 1, e deve, pertanto, essere oggetto di stretta interpretazione, considerate le responsabilità anche sul piano penale che possono derivare dalla violazione del predetto quadro normativo. Per scelta espressa del legislatore, solo gli strumenti preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla "registrazione

degli accessi e delle presenze" e allo "svolgimento della prestazione" non soggiacciono quindi ai limiti e alle garanzie di cui al primo comma, in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa.

Alla luce delle disposizioni richiamate, affinché sia ritenuto applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'attività di raccolta e conservazione dei soli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, si ritiene che possa essere effettuata, di norma, per un periodo limitato a pochi giorni; a titolo orientativo, tale conservazione non dovrebbe comunque superare i 21 giorni. Sempre nell'ambito della predetta finalità (assicurare il funzionamento delle infrastrutture del sistema della posta elettronica), a cui risulta applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability previsto dall'art. 5, par. 2, del Regolamento, le specificità della realtà tecnica e organizzativa del titolare. Spetta in ogni caso al titolare adottare tutte le misure tecniche ed organizzative per assicurare il rispetto del principio di limitazione della finalità, l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti e la tracciatura degli accessi effettuati.

Diversamente, la generalizzata raccolta e la conservazione dei log di posta elettronica, per un lasso di tempo più esteso, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta L. n. 300/1970 (v., da ultimo, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530). Resta fermo che anche tale conservazione dovrà avvenire nel rispetto del principio di limitazione della conservazione (v. successivo punto 4.2).

4. Le possibili responsabilità per i datori di lavoro pubblici e privati

4.1 Liceità del trattamento

Con riferimento alla liceità del trattamento, si precisa in primo luogo che il ricorso a sistemi e soluzioni di gestione e conservazione dei log delle comunicazioni elettroniche (come definiti più sopra nel documento) può considerarsi rientrante nell'eccezione di cui al comma 2 dell'art. 4, L. n. 300/1970 nei casi, alle condizioni e per le finalità già richiamate nel precedente par. 3.

Altri profili di illiceità possono poi derivare dall'utilizzo ulteriore dei dati personali, raccolti in assenza delle predette garanzie. Ciò in quanto l'art. 4, comma 3, della L. n. 300/1970 consente di utilizzare, per le finalità connesse alla gestione del rapporto di lavoro, solo le informazioni già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dai commi 1 e 2 e, dunque, nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata nonché fornendo una "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli" nel rispetto di quanto disposto dalla disciplina di protezione dei dati personali (cfr. provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 13 maggio 2021, n. 190, doc. web n. 9669974).

Inoltre, dagli elementi ricavabili dai dati esteriori della corrispondenza, come l'oggetto, il mittente e il destinatario e altre informazioni che accompagnano i dati in transito, definendone profili temporali (come la data e l'ora di invio/ricezione), nonché dagli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto (in quanto anche questi dati sono, a propria volta, suscettibili di aggregazione, elaborazione e di controllo), è possibile acquisire informazioni riferite alla sfera personale o alle opinioni dell'interessato.

Sotto tale profilo, si ricorda che, fin dal 1970, al datore di lavoro pubblico e privato è fatto divieto di "effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del

lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" (v. art. 8 della L. n. 300/1970 e art. 10 del d.lgs. 10 settembre 2003, n. 276, richiamati espressamente dall'art. 113 del Codice). La generalizzata raccolta e la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per un periodo di tempo esteso, in assenza di idonei presupposti giuridici, può, dunque comportare la possibilità per il datore di lavoro di acquisire, informazioni riferite alla sfera personale o alle opinioni dell'interessato e quindi non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

4.2 Principio di correttezza e trasparenza

In ogni caso, si richiamano tutti i titolari del trattamento a verificare che la raccolta e la conservazione dei log avvengano nel rispetto dei principi di correttezza e trasparenza nei confronti dei lavoratori e che i lavoratori siano stati adeguatamente informati sul trattamento dei dati personali relativi alle comunicazioni elettroniche che li riguardano (cfr. artt. 5, par. 1, lett. a), 12, 13 e 14 del Regolamento).

A questo proposito è essenziale che gli interessati siano resi pienamente consapevoli delle complessive caratteristiche del trattamento (specificando i tempi di conservazione dei dati, gli eventuali controlli, ecc.).

4.3 Principio di limitazione della conservazione

I tempi di conservazione dei metadati devono in ogni caso essere proporzionati rispetto alle legittime finalità perseguite. In particolare, finalità connesse alla sicurezza informatica e alla tutela del patrimonio informatico giustificano la conservazione dei metadati per un arco temporale congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure. Ove i tempi di conservazione non siano definiti in maniera proporzionata alle finalità del trattamento, il titolare del trattamento può incorrere nella violazione del principio di "limitazione della conservazione" (art. 5, par. 1, lett. e), del Regolamento).

4.4 Principi di protezione dei dati fin dalla progettazione e per impostazione predefinita e principio di responsabilizzazione

Il datore di lavoro deve, altresì, adottare misure volte ad assicurare il rispetto dei principi della protezione dei dati fin dalla progettazione del trattamento e per impostazione predefinita (art. 25 del Regolamento) durante l'intero ciclo di vita dei dati, "incorporan[d]o nel trattamento le misure e le garanzie adeguate ad assicurare l'efficacia dei principi di protezione dei dati, dei diritti e delle libertà degli interessati" e facendo in modo che "[venga] effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire la specifica e lecita finalità", anche con riguardo al periodo di conservazione dei dati, "in tutte le fasi della progettazione delle attività di trattamento, compresi gli appalti, le gare di appalto, l'esternalizzazione, lo sviluppo, il supporto, la manutenzione, il collaudo, la conservazione, la cancellazione ecc." ("Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020).

Inoltre, considerando che sul titolare del trattamento, in quanto soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, grava una "responsabilità generale" sui trattamenti posti in essere (cons. 74 del Regolamento; cfr., tra i tanti, provv. 10 febbraio 2022, n. 43, doc. web n. 9751498 e i precedenti provv. ivi richiamati; v. anche le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. par. 174), i trattamenti in questione possono comportare anche la violazione del principio di "responsabilizzazione" (artt. 5, par. 1, e 24 del Regolamento), in base al quale il titolare è tenuto a

rispettare i principi di protezione dei dati (art. 5, par. 1, del Regolamento) e deve essere in grado di comprovarlo (art. 5, par. 2, del Regolamento). Ciò anche con riguardo alle adeguate misure tecniche e organizzative messe in atto al fine di garantire il rispetto della disciplina in materia di protezione dei dati e di quella di settore eventualmente applicabile (art. 24, par. 1, del Regolamento).

Come recentemente messo in evidenza dal Garante, il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del Responsabile della protezione dei dati, ove designato, la conformità ai principi applicabili al trattamento dei dati (art. 5 del Regolamento) adottando, nel rispetto del principio di responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 del Regolamento; cfr., con riguardo a specifici trattamenti in ambito lavorativo, provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 10 giugno 2021, n. 235, doc. web n. 9685922; ma v. anche provv. 17 dicembre 2020, n. 282, doc. web n. 9525337). Il titolare del trattamento deve quindi accertare che siano disattivate le funzioni che non sono compatibili con le proprie finalità del trattamento o che si pongono in contrasto con specifiche norme di settore previste dall'ordinamento ad esempio commisurando adeguatamente anche i tempi di conservazione dei dati ovvero chiedendo al fornitore del servizio di anonimizzare i metadati raccolti nei casi in cui non si intenda effettuare una conservazione più prolungata degli stessi.

4.4.1. I principi di protezione dei dati fin dalla progettazione e per impostazione predefinita e i fornitori dei servizi di posta elettronica

In tale prospettiva, il Regolamento prevede che, già in fase di progettazione, sviluppo, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali, i produttori dei servizi e delle applicazioni debbano tenere conto del diritto alla protezione dei dati conformemente allo stato dell'arte.

Anche i fornitori, pertanto, devono contribuire a far sì che i titolari del trattamento possano adempiere ai loro obblighi di protezione dei dati, contemperando le esigenze di commercializzazione su larga scala dei propri prodotti con la conformità degli stessi ai principi del Regolamento, anche nella prospettiva di migliorare il prodotto offerto, sotto il profilo della sua maggiore conformità al Regolamento (v. cons. 78 del Regolamento).

5. Le iniziative da porre in essere per assicurare il rispetto della normativa in materia di protezione dei dati e la disciplina di settore in materia di controlli a distanza

Alla luce delle considerazioni che precedono e al fine di prevenire trattamenti di dati personali non conformi al richiamato quadro normativo, con conseguenti responsabilità sul piano sia amministrativo che penale, i datori di lavoro pubblici e privati dovranno adottare le misure necessarie a conformare i propri trattamenti alla disciplina di protezione dati e a quella di settore.

In particolare, spetta al titolare del trattamento verificare che i programmi e servizi informatici di gestione della posta elettronica in uso ai dipendenti - specialmente nel caso in cui si tratti di prodotti di mercato forniti in modalità cloud o as-a-service - consentano al cliente (datore di lavoro) di rispettare la disciplina di protezione dei dati nei termini indicati nel presente documento di indirizzo, anche con riguardo al periodo di conservazione dei metadati secondo quanto indicato al par. 3.

Da ultimo, si fa presente che le indicazioni di cui al presente documento di indirizzo devono considerarsi valide anche nel caso in cui, in ambito pubblico, i programmi e servizi informatici in questione siano acquistati mediante le convenzioni/piattaforme che le pubbliche amministrazioni devono o possono utilizzare per l'acquisto di beni e servizi.

In ogni caso, con riferimento all'utilizzo di servizi basati sul cloud nel settore pubblico, si richiama quanto indicato nel report "2022 Coordinated Enforcement Action Use of cloud-based services by the public sector" del Comitato europeo per la protezione dei dati (adottato il 17 gennaio 2023, reperibile alla pagina web https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en), che reca indicazioni sulle misure tecniche e organizzative necessarie ad assicurare il rispetto del Regolamento in tale contesto, garantendo, in particolare, che i fornitori dei servizi cloud trattino i dati personali solo per conto dei rispettivi titolari e sulla base delle istruzioni da questi ricevute.

Provvedimento del 21 dicembre 2023 - Documento di indirizzo “Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati” [9978728]

VEDI ANCHE Newsletter del 6 febbraio 2024

[doc. web n. 9978728]

Provvedimento del 21 dicembre 2023 - Documento di indirizzo “Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”

Registro dei provvedimenti
n. 642 del 21 dicembre 2023

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, l'avv. Guido Scorza, componente e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, “Regolamento generale sulla protezione dei dati” (di seguito, “Regolamento”), con particolare riguardo agli artt. 5, 6 e 88 dello stesso;

VISTO il d.lgs. 30 giugno 2003, n. 196 recante “Codice in materia di protezione dei dati personali”, recante disposizioni per l’adeguamento dell’ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito “Codice”), con particolare riguardo agli artt. 113 e 114 dello stesso;

VISTI gli artt. 4 e 8 della l. 20 maggio 1970, n. 300, nonché l’art. 10 del d.lgs. 10 settembre 2003, n. 276;

CONSIDERATO che nell’ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica, commercializzati da fornitori in modalità cloud, possano raccogliere, per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all’utilizzo degli account di posta elettronica in uso ai dipendenti (ad esempio, giorno, ora, mittente, destinatario, oggetto e dimensione dell’email), conservando gli stessi per un esteso arco temporale; ciò talvolta ponendo, altresì, limitazioni al cliente (datore di lavoro) in ordine alla possibilità di modificare le impostazioni di base del programma informatico al fine di disabilitare la

raccolta sistematica di tali dati o di ridurre il periodo di conservazione degli stessi;

CONSIDERATO che il Garante ha il compito di promuovere la consapevolezza e la comprensione del pubblico, dei titolari e dei responsabili del trattamento riguardo a norme, obblighi, rischi, garanzie e diritti stabiliti dal Regolamento (ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento);

CONSIDERATO che il Garante ha il potere di adottare documenti di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento anche per singoli settori o in applicazione dei principi di cui all'articolo lo 25 del Regolamento (art. 154-bis, comma 1, lett. a) del Codice);

RITENUTO, pertanto, di dover adottare l'allegato Documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" (all. n. 1), che forma parte integrante del presente provvedimento, volto a fornire talune indicazioni ai datori di lavoro pubblici e privati e agli altri soggetti a vario titolo coinvolti, al fine di promuovere la consapevolezza delle scelte, anche organizzative, dei titolari del trattamento, nonché a prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la liberà e la dignità dei lavoratori (cfr. artt. 113 e 114 del Codice), favorendo, in tal modo, la più ampia comprensione riguardo alle norme e alle garanzie che devono essere rispettate nel contesto lavorativo, tenuto conto degli elevati rischi per i diritti e le libertà degli interessati;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

RELATORE l'avv. Guido Scorza;

TUTTO CIÒ PREMESSO

adotta, ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento nonché ai sensi dell'art. 154-bis, c.1, lett. a) del Codice, il documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" (all. n. 1), che forma parte integrante del presente provvedimento, volto a fornire talune indicazioni ai datori di lavoro pubblici e privati e agli altri soggetti a vario titolo coinvolti, al fine di promuovere la consapevolezza delle scelte, anche organizzative, dei titolari del trattamento, nonché a prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la liberà e la dignità dei lavoratori (cfr. artt. 113 e 114 del Codice), favorendo, in tal modo, la più ampia comprensione riguardo alle norme e alle garanzie che devono essere rispettate nel contesto lavorativo, tenuto conto degli elevati rischi per i diritti e le libertà degli interessati.

Roma, 21 dicembre 2023

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei

DOCUMENTO DI INDIRIZZO

Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati

1. Introduzione

Nell'ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica, commercializzati da fornitori in modalità cloud, possano raccogliere per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti (ad esempio, giorno, ora, mittente, destinatario, oggetto e dimensione dell'email), conservando gli stessi per un esteso arco temporale. Ciò talvolta ponendo, altresì, limitazioni al cliente (datore di lavoro) in ordine alla possibilità di modificare le impostazioni di base del programma informatico al fine di disabilitare la raccolta sistematica di tali dati o di ridurre il periodo di conservazione degli stessi.

2. La normativa in materia di protezione dei dati personali

Come costantemente affermato dal Garante, il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.), che proteggono il nucleo essenziale della dignità della persona e il pieno sviluppo della sua personalità nelle formazioni sociali. Ciò comporta che, anche nel contesto lavorativo pubblico e privato, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza (v. punto 5.2 lett. b), delle "Linee guida del Garante per posta elettronica e Internet" del 1° marzo 2007, n. 13, doc. web n. 1387522; cfr., tra i tanti, provv. 4 dicembre 2019, n. 216, doc. web n. 9215890 e i precedenti in esso citati).

Considerato che l'impiego dei predetti programmi e servizi informatici dà luogo a "trattamenti" di dati personali, riferiti a "interessati", identificati o identificabili (art. 4, par. 1, nn. 1) e 2), del Regolamento) nel contesto lavorativo, è necessario che il datore di lavoro, in quanto titolare del trattamento, verifichi la sussistenza di un idoneo presupposto di liceità (cfr. artt. 5, par. 1, lett. a) e 6 del Regolamento) prima di effettuare trattamenti di dati personali dei lavoratori attraverso tali programmi e servizi, rispettando le condizioni per il lecito impiego di strumenti tecnologici nel contesto lavorativo (art. 88, par. 2, del Regolamento).

In particolare, dovrà quindi essere sempre verificata la sussistenza dei presupposti di liceità stabiliti dall'art. 4 della l. 20 maggio 1970, n. 300, cui fa rinvio l'art. 114 del Codice, nonché il rispetto delle diposizioni che vietano al datore di lavoro di acquisire e comunque trattare informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o comunque afferenti alla sua sfera privata (art. 8 della l. 20 maggio 1970, n. 300 e art. 10 d.lgs. 10 settembre 2003, n. 276, cui fa rinvio l'art. 113 del Codice). Gli artt. 113 e 114 del Codice sono infatti considerati, nell'ordinamento italiano, disposizioni più specifiche e di maggiore garanzia di cui all'art. 88 del Regolamento, la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione determina, oltre all'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, par. 5, lett. d) del Regolamento, anche il possibile insorgere di responsabilità sul piano penale (cfr. art. 171 del Codice).

Il titolare del trattamento è inoltre tenuto a rispettare i principi generali del trattamento (artt. 5, 24 e 25 del Regolamento) e a porre in essere tutti gli adempimenti previsti dalle disposizioni normative

in materia di protezione dei dati personali (v. artt. 12, 13, 14, 30, 32 e 35 del Regolamento), anche con riguardo alla necessità di fornire agli interessati in modo corretto e trasparente una chiara rappresentazione del complessivo trattamento effettuato, consentendo agli stessi di disporre di tutti gli elementi informativi essenziali previsti dal Regolamento e di essere pienamente consapevole, prima che il trattamento abbia inizio, delle caratteristiche dello stesso (cfr. sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. par. n. 133 e 140).

Inoltre, in attuazione del principio di "responsabilizzazione" (cfr. art. 5, par. 2, e 24 del Regolamento), spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche - in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite - che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali (cfr. cons. 90 e artt. 35 e 36 del Regolamento).

Anche tenuto conto delle indicazioni fornite anche a livello europeo sul punto, tale necessità ricorre, in particolare, in caso di raccolta e memorizzazione dei metadati relativi all'impiego della posta elettronica, stante la particolare "vulnerabilità" degli interessati nel contesto lavorativo, nonché il rischio di "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti" (Gruppo di lavoro art. 29, "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento", WP 248 del 4 aprile 2017; cfr. cons. 75 e artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1; v., tra gli altri, provv. 13 maggio 2021, n. 190, doc. web n. 9669974, par. 3.5).

3. La disciplina di settore in materia di controlli a distanza

L'art. 4, comma 1, l. 20 maggio 1970, n. 300, come modificato dal d.lgs. 14 settembre 2015, n. 151, individua tassativamente le finalità (ovvero quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) 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 (accordo sindacale o autorizzazione pubblica).

Le predette garanzie non trovano invece applicazione "agli strumenti di registrazione degli accessi e delle presenze", così come "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970). Tale disposizione introduce un'eccezione, rispetto al più restrittivo regime previsto dal comma 1, e deve, pertanto, essere oggetto di stretta interpretazione, considerate le responsabilità anche sul piano penale che possono derivare dalla violazione del predetto quadro normativo. Per scelta espressa del legislatore, solo gli strumenti preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla "registrazione degli accessi e delle presenze" e allo "svolgimento della prestazione" non soggiacciono quindi ai limiti e alle garanzie di cui al primo comma, in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa.

Alla luce delle disposizioni richiamate, l'attività di raccolta e conservazione dei soli c.d. metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, per un tempo che, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione - affinché sia ritenuto applicabile il comma 2 dell'art. 4 della L. n. 300/1970 – non può 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 giustifichino il prolungamento, di ulteriori 48 ore (v. provv.ti nn. 303 del 13 luglio 2016, doc. web n. 5408460; 1° febbraio 2018, n. 53, doc. web n. 8159221; 29 ottobre 2020, n. 214, doc. web n. 9518890; 29 settembre 2021, n. 353, doc. web n. 9719914).

Diversamente, la generalizzata raccolta e la conservazione di tali metadati, per un lasso di tempo più esteso – ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro -, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta l. n. 300/1970 (v., da ultimo, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530). Resta fermo che anche tale conservazione dovrà avvenire nel rispetto del principio di limitazione della conservazione (v. successivo punto 4.2.).

4. Le possibili responsabilità per i datori di lavoro pubblici e privati

4.1 Illiceità del trattamento

In considerazione del richiamato quadro giuridico, l'impiego dei predetti programmi e servizi di gestione della posta elettronica, in assenza dell'espletamento delle procedure di garanzia di cui all'art. 4, comma 1, della l. n. 300/1970, prima di dare avvio alla preventiva e sistematica raccolta dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, e alla conservazione degli stessi per un ampio arco temporale (superiore a sette giorni estensibili di ulteriori 48 ore , alle condizioni indicate al par. 3), si pone in contrasto con la normativa in materia di protezione dei dati personali e con la richiamata disciplina di settore, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970).

Altri profili di illiceità possono poi derivare dall'utilizzo ulteriore dei dati personali, raccolti in assenza delle predette garanzie. Ciò in quanto l'art. 4, comma 3, consente di utilizzare, per le finalità connesse alla gestione del rapporto di lavoro, solo le informazioni già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dai commi 1 e 2 e, dunque, nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata (cfr. provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 13 maggio 2021, n. 190, doc. web n. 9669974).

Inoltre, dagli elementi ricavabili dai dati esteriori della corrispondenza, come l'oggetto, il mittente e il destinatario e altre informazioni che accompagnano i dati in transito, definendone profili temporali (come la data e l'ora di invio/ricezione), nonché dagli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto (in quanto anche questi dati sono, a propria volta, suscettibili di aggregazione, elaborazione e di controllo), è possibile acquisire informazioni riferite alla sfera personale o alle opinioni dell'interessato.

Sotto tale profilo, si ricorda che, fin dal 1970, al datore di lavoro pubblico e privato è fatto divieto di "effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" (v. art. 8 della l. n. 300/1970 e art. 10 del d.lgs. 10 settembre 2003, n. 276, richiamati espressamente dall'art. 113 del Codice). La generalizzata raccolta e la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per un periodo di tempo esteso, in assenza di idonei presupposti giuridici, può, dunque comportare la possibilità per il datore di lavoro di acquisire, informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

4.2 Violazione del principio di limitazione della conservazione

I tempi di conservazione dei metadati devono in ogni caso essere proporzionati rispetto alle legittime finalità perseguite. In particolare, finalità connesse alla sicurezza informativa e alla tutela del patrimonio informativa giustificano la conservazione dei metadati per un arco temporale congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure. Ove i tempi di conservazione non siano definiti in maniera proporzionata alle finalità del trattamento, il titolare del trattamento può incorrere nella

violazione del principio di “limitazione della conservazione” (art. 5, par. 1, lett. e), del Regolamento).

4.3 Violazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, e di responsabilizzazione

Il datore di lavoro deve, altresì, adottare misure volte ad assicurare il rispetto dei principi della protezione dei dati fin dalla progettazione del trattamento e per impostazione predefinita (art. 25 del Regolamento) durante l’intero ciclo di vita dei dati, “incorporan[d]o nel trattamento le misure e le garanzie adeguate ad assicurare l’efficacia dei principi di protezione dei dati, dei diritti e delle libertà degli interessati” e facendo in modo che “[venga] effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire la specifica e lecita finalità”, anche con riguardo al periodo di conservazione dei dati, “in tutte le fasi della progettazione delle attività di trattamento, compresi gli appalti, le gare di appalto, l’esternalizzazione, lo sviluppo, il supporto, la manutenzione, il collaudo, la conservazione, la cancellazione ecc.” (“Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020).

Inoltre, considerando che sul titolare del trattamento, in quanto soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, grava una “responsabilità generale” sui trattamenti posti in essere (cons. 74 del Regolamento; cfr., tra i tanti, provv. 10 febbraio 2022, n. 43, doc. web n. 9751498 e i precedenti provv. ivi richiamati; v. anche le “Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR”, adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. par. 174), i trattamenti in questione possono comportare anche la violazione del principio di “responsabilizzazione” (artt. 5, par. 1, e 24 del Regolamento), in base al quale il titolare è tenuto a rispettare i principi di protezione dei dati (art. 5, par 1, del Regolamento) e deve essere in grado di comprovarlo (art. 5, par. 2, del Regolamento). Ciò anche con riguardo alle adeguate misure tecniche e organizzative messe in atto al fine di garantire il rispetto della disciplina in materia di protezione dei dati e di quella di settore eventualmente applicabile (art. 24, par. 1, del Regolamento).

Come, infatti, recentemente messo in evidenza dal Garante, il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del Responsabile della protezione dei dati, ove designato, la conformità ai principi applicabili al trattamento dei dati (art. 5 del Regolamento) adottando, nel rispetto del principio di responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 del Regolamento; cfr., con riguardo a specifici trattamenti in ambito lavorativo, provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 10 giugno 2021, n. 235, doc. web n. 9685922; ma v. anche provv. 17 dicembre 2020, n. 282, doc. web n. 9525337). In tale prospettiva, il titolare del trattamento deve accertarsi, ad esempio, che siano disattivate le funzioni che non sono compatibili con le finalità del trattamento o che si pongono in contrasto con specifiche norme di settore previste dall’ordinamento, specie in ambito lavorativo, commisurando adeguatamente anche i tempi di conservazione dei dati.

5. Le iniziative da porre in essere per assicurare il rispetto della normativa in materia di protezione dei dati e la disciplina di settore in materia di controlli a distanza

Alla luce delle considerazioni che precedono e al fine di prevenire trattamenti di dati personali non conformi al richiamato quadro normativo, con conseguenti responsabilità sul piano sia amministrativo che penale, i datori di lavoro pubblici e privati dovranno adottare le misure necessarie a conformare i propri trattamenti alla disciplina di protezione dati e a quella di settore.

In particolare, si rende necessario verificare con la dovuta diligenza che i programmi e servizi

informatici di gestione della posta elettronica in uso ai dipendenti - specialmente nel caso in cui si tratti di prodotti di mercato forniti in modalità cloud o as-a-service - consentano al cliente (datore di lavoro) di modificare le impostazioni di base, impedendo la raccolta dei predetti metadati o limitando il periodo di conservazione degli stessi ad un limite massimo di sette giorni, estensibile di ulteriori 48 ore, alle condizioni indicate al par. 3.

In tale prospettiva, si invitano i produttori dei servizi e delle applicazioni, in fase di sviluppo e progettazione degli stessi, a tenere conto del diritto alla protezione dei dati tenuto conto dello stato dell'arte (v. cons. 78 del Regolamento).

Diversamente, i datori di lavoro pubblici o privati, in qualità di titolari del trattamento, dovranno alternativamente, nel caso in cui i trattamenti di dati personali in questione si dovessero comunque rendere necessari per il perseguimento di esigenze organizzative o produttive, espletare le richiamate procedure di garanzia previste dalla disciplina di settore (art. 4 della l. 300/1970) o cessare l'utilizzo di tali programmi e servizi informatici. Resta inteso che, nelle more dell'eventuale espletamento delle procedure di garanzia, i predetti metadati non possono comunque essere utilizzati (cfr. art. 2-decies del Codice).

In ogni caso, deve essere assicurata la necessaria trasparenza nei confronti dei lavoratori, fornendo agli stessi una specifica informativa sul trattamento dei dati personali prima di dare inizio al trattamento (cfr. art. 5, par. 1, lett. a), 12 e 13 del Regolamento). Ciò anche tenuto conto del fatto che l'adempimento degli obblighi informativi nei confronti dei dipendenti (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce anche una specifica precondizione per il lecito utilizzo dei dati raccolti attraverso strumenti tecnologici, da parte del datore di lavoro, anche a tutti i fini connessi al rapporto di lavoro (art. 4, co. 3, della l. n. 300/1970).

Da ultimo, si fa presente che le indicazioni di cui al presente documento di indirizzo devono considerarsi valide anche nel caso in cui, in ambito pubblico, i programmi e servizi informatici in questione siano acquistati mediante le convenzioni/piattaforme che le pubbliche amministrazioni devono o possono utilizzare per l'acquisto di beni e servizi.

In ogni caso, con riferimento all'utilizzo di servizi basati sul cloud, si richiama quanto indicato nel report "2022 Coordinated Enforcement Action Use of cloud-based services by the public sector" del Comitato europeo per la protezione dei dati (adottato il 17 gennaio 2023, reperibile alla pagina web https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en), che reca indicazioni sulle misure tecniche e organizzative necessarie ad assicurare il rispetto del Regolamento in tale contesto, garantendo, in particolare, che i fornitori dei servizi cloud trattino i dati personali solo per conto dei rispettivi titolari e sulla base delle istruzioni da questi ricevute.