NEWS

E-mail dei dipendenti: arriva il documento di indirizzo del Garante della Privacy

Data pubblicazione: 16/02/2024

Autore: Admin

Contenuto

Con provvedimento del 21 dicembre 2023, il Garante privacy per la gestione della posta elettronica e dei metadati dei lavoratori ha fornito importanti linee guida. Il provvedimento del Garante, infatti, ha fissato dei vincoli molto restrittivi, stabilendo che i datori di lavoro non possono conservare i metadati delle email dei dipendenti (data, ora, mittente, destinatario, oggetto e dimensione) posizionati su cloud esterni oltre un periodo di tempo estremamente breve. Qui di seguito il documento di indirizzo adottato.

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.