Spett.le Garante per la protezione dei dati personali

Piazza Venezia, n. 11

00187- Roma

protocollo@gpdp.it - protocollo@pec.gpdp.it

Oggetto: risposta alla consultazione pubblica avviata dal Garante per la protezione dei dati personali sul termine di conservazione dei metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica (G.U. - Serie Generale n. 64 del 16 marzo 2024)

Con il presente documento, ABI - Associazione Bancaria Italiana, ANIA - Associazione Nazionale fra le Imprese di Assicurazione, Confcommercio Imprese per l'Italia e Confindustria (di seguito, congiuntamente "**Associazioni**") intendono formulare alcune considerazioni in risposta alla consultazione opportunamente avviata sul Provvedimento del Garante per la protezione dei dati personali del 21 dicembre 2023, n. 642, recante "*Documento di indirizzo Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*" (di seguito, "**Provvedimento**"), la cui efficacia è stata temporaneamente sospesa.

Con il Provvedimento, il Garante per la protezione dei dati personali (di seguito, anche "**Garante**" o "**Autorità**") ha fornito indicazioni sulla conservazione dei c.d. metadati degli *account* dei servizi di posta elettronica aziendali in uso ai lavoratori, identificandoli – con un'esemplificazione – nel giorno, ora, mittente, destinatario, oggetto e dimensione dell'e-mail.

In particolare, il Provvedimento, in prima istanza, riconosce – ai fini dell'art. 4, comma 2 della legge 300/1970 (di seguito, "**Statuto dei lavoratori**") – la valenza di "strumento di lavoro" della posta elettronica e dei correlati c.d. metadati.

Peraltro, precisa che trascorso un periodo di 7 giorni (estendibili di ulteriori 48 ore, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento) i soli metadati devono essere cancellati, salva in alternativa l'attivazione delle procedure previste dall'art. 4, comma 1, dello Statuto dei lavoratori.

Ad avviso dell'Autorità, infatti, la raccolta e la conservazione dei metadati possono considerarsi attività necessarie ad "*assicurare il funzionamento delle infrastrutture del sistema della posta elettronica"* e, quindi, lecite *ex* art. 4, comma 2, dello Statuto dei lavoratori, solo se realizzate per un arco temporale limitato.

Diversamente, la raccolta e la conservazione dei metadati per un lasso di tempo maggiore dovrebbero considerarsi funzionali al perseguimento di altre finalità – es. sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro – e, **"***potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori",* sarebbero lecite solo previo esperimento delle garanzie stabilite dall'art. 4, comma 1, dello Statuto dei lavoratori.

Le scriventi Associazioni, raccogliendo le osservazioni e le istanze delle proprie associate – tra cui le più importanti imprese tecnologiche italiane, nonché filiali italiane di importanti multinazionali – devono esprimere un motivato dissenso rispetto alle predette valutazioni relative all'applicazione dell'art. 4 dello Statuto dei lavoratori alla posta elettronica e ai correlati metadati, ferma restando l'esigenza e la consapevolezza della necessità di prestare particolare attenzione, in ambito lavorativo, al principio di limitazione della conservazione, in base alle finalità per cui i dati personali sono trattati.

Ad avviso delle scriventi Associazioni, assume valenza centrale e dirimente la qualificazione dei metadati come "strumento di lavoro", nel senso di cui alla previsione dell'art. 4, comma 2, dello Statuto dei lavoratori.

Si osserva sul punto che, anche se si volesse accedere alla definizione (*rectius* esemplificazione) di metadato fornita nel Provvedimento, la sua riconducibilità alla fattispecie di cui all'art. 4, comma 1, dello Statuto dei lavoratori non appare in linea con la lettera e la struttura complessiva della norma e, in particolare, con la disciplina che la stessa prescrive per gli "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"* e per l'utilizzo delle "*informazioni raccolte"* dagli stessi.

Come noto, infatti, l'art. 4, comma 2, dello Statuto dei lavoratori introduce una deroga alla procedura concertativo-autorizzativa di cui al 1° comma per gli impianti e gli strumenti che, sebbene possano comportare un controllo a distanza sull'attività dei lavoratori, sono da questi ultimi utilizzati "*per rendere la prestazione lavorativa".*

Dunque, l'operatività dell'art. 4, comma 2, dello Statuto dei lavoratori è determinata dalla qualificazione del predetto sistema o impianto quale **strumento di lavoro**, anche in ragione delle caratteristiche tecniche di configurazione.

Ebbene, in primo luogo, quelli che l'Autorità individua come metadati non possono essere classificati e autonomamente considerati come "strumenti" (termine impiegato nell'art. 4, comma, 1 dello Statuto dei lavoratori).

I dati esemplificativamente indicati nel provvedimento (giorno, ora, mittente, destinatario, oggetto e dimensione dell'e-mail) sono infatti parte costitutiva delle e-mail stesse e la loro cancellazione *tout court* determinerebbe la cancellazione delle e-mail (o quantomeno di loro parti essenziali).

Si tratta, quindi, di dati insiti e connaturati ad uno "strumento", qual è quello della posta elettronica complessivamente considerata data in uso ai lavoratori che, pacificamente, è indispensabile per rendere la prestazione lavorativa, in base alla definizione di "strumento di lavoro" fornita dalle Autorità competenti (*cfr*. Circ. Ispettorato Nazionale del Lavoro n. 2 del 2016; *ex multis* Tribunale di Roma, sentenza del 24/03/2017).

Da ciò consegue che la raccolta e la conservazione dei metadati devono necessariamente essere disciplinate in modo uniforme rispetto a quanto previsto per lo strumento di provenienza (*id est* il sistema di posta elettronica) e, quindi, **trovano, in ogni caso, il proprio presupposto di liceità nell'art. 4, comma 2, dello Statuto dei lavoratori**.

Ritenere, invero, che la posta elettronica costituisca uno strumento utilizzato dal lavoratore per rendere la prestazione lavorativa, ma che i metadati conservino tale connotazione solo nel momento del loro immediato utilizzo e, al più, per 7/9 giorni successivi (perdendola dopo questo limite temporale) è una conclusione che, sulla base degli ampi e complessi confronti

avuti con tutte le imprese tecnologicamente più avanzate del nostro Paese, non ha un fondamento tecnico.

Ciò in quanto, proprio dai confronti tecnici di cui si diceva, è emerso che l'archiviazione delle e-mail, compresi i dati esteriori, è assolutamente necessaria per il normale svolgimento di qualsiasi attività lavorativa che comporti l'utilizzo della posta elettronica.

Nello specifico, quelli che il Garante definisce come metadati sono indispensabili all'indicizzazione e alla gestione delle e-mail, ne consentono l'invio, la ricezione, la ricerca,

la classificazione (anche rispetto alle etichette di riservatezza) e la conservazione, garantendone al contempo integrità e accessibilità.

È un dato di realtà ineludibile quello per cui qualsiasi lavoratore che impieghi normalmente lo strumento della posta elettronica per rendere la propria prestazione utilizzi quotidianamente i metadati per la ricerca veloce ed intelligente delle comunicazioni ricevute ed inviate nel tempo.

Ne consegue che **i metadati assolvono, in ogni tempo e fase** (anche ben oltre il decorso dei predetti 7/9 giorni), **una funzione necessaria al normale svolgimento di qualsiasi attività lavorativa che comporti l'impiego della posta elettronica** e, pertanto, devono essere considerati preordinati allo svolgimento dell'attività lavorativa, ai sensi dell'art. 4, co. 2 dello Statuto dei lavoratori.

Ciò premesso, occorre evidenziare ulteriori profili di attenzione rispetto alle indicazioni contenute nel Provvedimento.

Anzitutto, va ricordato che in base all'art. 4, comma 1, dello Statuto dei lavoratori, per quei sistemi che non si configurano come "strumenti di lavoro", l'accordo sindacale o l'autorizzazione amministrativa devono perfezionarsi **prima** dell'installazione dello strumento da cui possa potenzialmente derivare un controllo dei lavoratori.

La disposizione, infatti, si fonda su un presupposto logico per cui, una volta che il sistema viene classificato o meno come strumento di lavoro, non è il decorso del tempo che può modificare la sua natura.

In secondo luogo, occorre evidenziare che nel Provvedimento **non appare una definizione precisa di metadati**. Conseguentemente, il concetto di metadato – anche tenendo conto di quanto esplicitato nell'avviso di avvio della consultazione – risulta ancora **troppo generico e poco chiaro, sia dal punto di vista tecnico, che giuridico**.

Considerando che la fattispecie di cui all'art. 4, comma 1, dello Statuto dei lavoratori (cui il Garante riconduce la conservazione dei metadati per un periodo superiore a 7/9 giorni) assume rilevanza penale ai sensi dell'art. 171 del D. Lgs. n. 196/2003, c.d. Codice Privacy, l'assenza di una nozione puntuale e, soprattutto, di una definizione di legge di "metadato", prodotto dai sistemi di posta elettronica, rischia di confliggere con i principi costituzionali di legalità e della riserva di legge, in base ai quali il precetto sanzionato penalmente deve essere riconoscibile, in quanto individuato tassativamente, in modo puntuale e all'interno di una norma di legge.

Rispetto alla raccolta e alla conservazione dei metadati, infatti, la valutazione sul disvalore della condotta del datore di lavoro, da cui deriverebbe la sanzione penale, sarebbe non solo rimessa alla definizione di una fonte di rango sub-legislativo - quale è il Provvedimento - ma

anche priva di ogni determinatezza e tassatività, avendo il Provvedimento definito i metadati mediante una mera "esemplificazione".

Inoltre, l'applicazione della fattispecie dell'art. 4, comma 1, all'ipotesi di conservazione dei metadati per un periodo superiore a 7/9 giorni rischia anche di porsi in contrasto con il divieto di interpretazione analogica *in malam partem*, sancito dall'art. 14 delle Preleggi e dall'art. 1 Cod. Pen., e fondato, a livello costituzionale, sul principio di legalità di cui all'art. 25, comma 2, della Costituzione, oltre che integrare, in via generale, una interpretazione analogica in assenza di una lacuna normativa.

Infatti, tale operazione ermeneutica finirebbe per assoggettare una fattispecie, pacificamente regolata dall'art. 4, comma 2, dello Statuto dei lavoratori, all'applicazione dell'art. 4, comma 1, la cui violazione è, invece, sanzionata penalmente. Ciò in quanto, come argomentato in precedenza, i metadati non possono considerarsi come uno "strumento" autonomo e distinto da quello della posta elettronica.

Va altresì considerato che, con specifico rifermento ai tempi di conservazione dei metadati generati e raccolti dal sistema di posta elettronica per il suo funzionamento e relativi alla gestione del servizio infrastrutturale, nella disponibilità anche dei fornitori (c.d. metadati tecnici o metadati di trasporto), appare opportuno rappresentare che l'indicazione di un termine di conservazione pari a 7 giorni (anche nel caso di estensione per ulteriori 48 ore) non risulta coerente con le esigenze di sicurezza informatica. L'indicazione univocamente ricevuta dalle imprese associate è, infatti, che è necessario disporre dei metadati dalla scoperta dell'incidente informatico (il c.d. "Dwell Time", cioè il tempo in cui l'attaccante rimane in un ambiente vittima senza essere identificato che è di gran lunga superiore a quello indicato dall'Autorità). Ne consegue che non è possibile individuare un termine unico e trasversale di conservazione dei metadati, la cui definizione, come anticipato, va rimessa alla valutazione specifica del titolare del trattamento (ferma restando l'applicazione dell'art. 4, comma 2, dello Statuto dei lavoratori).

In ogni caso, poste queste necessarie precisazioni, le scriventi Associazioni sono, tuttavia, consapevoli dell'opportunità per il Garante di implementare **attività di sensibilizzazione** per evidenziare la necessità, in ambito lavorativo, di prestare particolare attenzione al rispetto, tra gli altri, del principio di limitazione della conservazione, promuovendo il ricorso agli strumenti di valutazione preliminare (c.d. DPIA) e di trasparenza nei confronti dei lavoratori.

Tale esigenza è assicurata dall'art. 4, comma 3, dello Statuto dei lavoratori che subordina l'utilizzo delle informazioni raccolte *ex multis* dagli strumenti di lavoro, al rispetto della normativa privacy e alla preventiva adeguata informazione dei lavoratori: pertanto è nella attuazione di tale previsione – e non del comma 1 – che deve essere assicurata la tutela della riservatezza dei lavoratori nell'utilizzo della posta elettronica aziendale, anche in base alle specifiche indicazioni che potranno essere elaborate dal Garante.

In un'ottica di *accountability* (principio di responsabilizzazione), su cui permea l'intera struttura del Regolamento Ue n. 679/2016 (di seguito, "**GDPR**") e si poggia la *compliance* in materia di protezione dei dati personali, si ritiene, tuttavia, che **non debba essere stabilito un termine di conservazione dei metadati** degli *account* dei servizi di posta elettronica dei lavoratori **unico e indistintamente applicabile a tutte le organizzazioni**.

In forza del principio di responsabilizzazione, infatti, spetta a ciascun datore di lavoro determinare, anche in ragione del contesto di riferimento e delle proprie specifiche e legittime esigenze gestionali (tra cui, anche la necessità di ottemperare a specifici obblighi normativi e principi generali[1]), un **termine di conservazione dei metadati proporzionato e congruo, che sia giustificabile in ragione delle finalità per le quali i dati personali sono trattati** (c.d. principio di limitazione della conservazione *ex* art. 5, par. 1, lett. e) del GDPR).

Inoltre, il principio di limitazione della conservazione richiede al titolare del trattamento non già di fissare una data di scadenza predeterminata alla conservazione dei dati in forma personale, quanto piuttosto di legare a una finalità la conservazione stessa: in altre parole, **la conservazione dei dati è lecita fintantoché la finalità alla quale la stessa è strettamente connessa risulta attuale** e spetta al titolare del trattamento fissare (oltre che dimostrare, laddove richiesto) i criteri e i termini temporali di conservazione dei dati.

Inoltre, come noto, l'*accountability* ha comportato la scomparsa dalla disciplina in materia di protezione dei dati personali di concetti quali "livello minimo" di misure di sicurezza tipici della Direttiva 95/46/CE e del Codice privacy precedente alle modifiche intervenute con il D. Lgs. n. 101/2018.

Pertanto, in questo senso, la determinazione di un congruo termine per la conservazione dei metadati non può essere lasciata a una decisione basata su *standard* fissi, ma deve essere il **risultato di un'analisi dettagliata del contesto operativo e dei rischi specifici associati al trattamento**.

Considerato infine che, anche in virtù delle Linee guida del Garante per posta elettronica e internet (Provvedimento 1° marzo 2007, n. 13), la maggior parte degli operatori ha da tempo adottato *policy* e regolamenti interni per disciplinare l'utilizzo della posta elettronica aziendale e che, naturalmente, mai contemplano generalizzate forme di controllo dell'attività dei lavoratori, si ritiene che possa essere questa la sede per un **approfondimento informativo sui metadati**, sulla relativa funzione nell'ambito dell'organizzazione e sulle finalità del loro trattamento, sulla durata della relativa conservazione, adottando un linguaggio chiaro e semplice, che possa favorirne la comprensione da parte di tutti i lavoratori.

Roma, 12 aprile 2024

Confindustria	**ABI**	**Ania**	**Confcommercio**
Direttore Generale	Direttore Generale	Direttore Generale	Segretario Generale
Raffaele Langella	Giovanni Sabatini	Dario Focarelli	

[1] In proposito, tra le normative che individuano obblighi di conservazione con tempistiche differenziate, si segnalano, a titolo esemplificativo, il disposto ex art. 2220 c.c., nonché le normative settoriali quali: i) quelle emanate dalle Autorità di vigilanza, ad esempio in materia di attività bancaria o assicurativa; ii) la disciplina di cui al Regolamento intermediari adottato con delibera Consob 20307 del 15 febbraio 2018; iii) DIRETTIVA (UE) 2022/2555, c.d. Direttiva NIS 2, in materia di sicurezza informatica.