AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

Spett.le
Autorità Garante per la Protezione dei Dati Personali
Piazza Venezia n.11
00186 ROMA
via PEC protocollo@gpdp.it

Oggetto: Consultazione pubblica Provvedimento dd-21/12/2003 – Note sulla conservazione dei metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica – Contributo

Spettabile Autorità,

con la presente si desidera contribuire alla consultazione pubblica rispetto alle indicazioni contenute Provvedimento dd.21/12/2023 e nel relativo Documento di Indirizzo attinenti al tempo di conservazione di 7 giorni (estensibili per ulteriori 48 ore in caso di comprovate esigenze) della raccolta automatizzata dei metadati degli account di posta elettronica messi a disposizione in ambito lavorativo (privato/pubblico) ed effettuata dai datori di lavoro per mezzo dei provider di posta elettronica.

Lo studio legale Ogriseg[1] affianca datori di lavoro privati e pubblici nonché dipendenti e collaboratori con particolare interesse per l'informatica giuridica. Composto da avvocati giuslavoristi specialisti in diritto del lavoro (con Dottorato di Ricerca in Diritto del Lavoro e Relazioni Industriali o con esame di Diritto del Lavoro al CNF), lo Studio legale Ogriseg sente particolarmente viva l'importanza di svolgere il ruolo che l'Ordinamento Costituzionale assegna agli avvocati: essere i custodi dell'effettività del diritto e della giurisdizione, in particolare nel diritto del lavoro. Come giuslavoristi i componenti dello studio considerano proprio dovere svolgere una verifica costante dell'efficacia della normazione, raccogliere e rappresentare le esigenze del mutamento, imposte dal rapido progredire della società e dell'economia, nella salvaguardia delle libertà e dei diritti a cui è preposto il sistema giuridico.

In simile prospettiva lo Studio legale Ogriseg ritiene di poter fornire alla consultazione pubblica indetta dall'Autorità Garante un punto di vista utile per una complessiva riflessione sulla gestione della posta elettronica, nell'ottica di una leale collaborazione e nella finalità di tutelare i beni giuridici coinvolti.

La posta elettronica aziendale è uno strumento di lavoro e i metadati fatti attinenti allo svolgimento dell'attività lavorativa

Analizzando lo sviluppo logico del ragionamento contenuto nel provvedimento dell'Autorità Garante Italiana, innanzitutto si osserva come la posta elettronica aziendale venga considerata "corrispondenza privata". Eppure simile approccio non considera che gli *account* di posta elettronica aziendale o dell'ente pubblico sono sempre uno strumento affidato per l'esecuzione della prestazione, da utilizzarsi per motivi lavorativi.

La posta elettronica fornita dal datore di lavoro per lo svolgimento dell'attività lavorativa è sempre uno strumento di lavoro. Uno strumento informatico adottato e affidato ai propri dipendenti/collaboratori per l'esercizio delle proprie funzioni talora di natura pubblicistica.

[1] Hanno collaborato alla stesura del presente documento l'avvocato Claudia Ogriseg, titolare dello studio legale e l'avvocato Alberto Tarlao.

AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

Nel contesto lavorativo l'affidamento a qualunque collaboratore di *account* di posta elettronica che consenta il collegamento a *internet*, comporta il potere/dovere del datore di lavoro di verificare il corretto e diligente utilizzo dello strumento affidato. Si tratta dell'esigenza di garantire, all'interno della propria organizzazione, il rispetto della normativa e di assicurare una effettiva tutela dei beni aziendali e di terzi. Gravano infatti sul datore di lavoro profili di responsabilità per un utilizzo *contra legem* dello strumento affidato al collaboratore.

Nell'ipotesi in cui l'*account* di posta elettronica sia generico ovvero non contenga alcuna generalità (nome e cognome del dipendente) ma si riferisca a un ufficio aziendale/pubblico (es. commerciale@..... acquisti@..... direzione@..... segreteria@..... etc.) è evidente che dovrà essere esclusa qualsivoglia legittima aspettativa del dipendente/collaboratore alla riservatezza della casella di posta elettronica in questione poiché pacificamente ad uso comune aziendale e/o dell'ente.

Analogamente, dovrà escludersi qualsivoglia legittima aspettativa di riservatezza del dipendente/collaboratore qualora l'*account* affidato dal datore di lavoro abbia un dominio aziendale e/o dell'ente, sia stato creato al solo e unico scopo di consentire lo svolgimento dell'attività lavorativa. L'utilizzo personale avulso da finalità lavorative dello strumento lavorativo dovrebbe essere sempre comunque vietato a qualunque collaboratore. In effetti, i più recenti approdi della giurisprudenza di legittimità (Cassazione sezione lavoro, sentenze n. 35643 e n.35644/2022) hanno considerato legittimo l'utilizzo della posta aziendale anche per comunicazioni sindacali esclusivamente considerata l'assenza di canali dedicati alle sole comunicazioni sindacali e sempre ed esclusivamente nel caso non creino pregiudizio all'azienda.

L'enorme diffusione degli *account* di posta elettronica e il loro utilizzo comune da parte delle persone comporta che solo e soltanto gli *account* di posta elettronica personali, creati dal dipendente in qualità di utente privato, possano essere assimilati alla corrispondenza privata e godere delle garanzie costituzionali di riservatezza e segretezza (artt.2 e 15 Cost.).

Sul punto, pare opportuno richiamare la recente sentenza n. 170/2023 della Corte Costituzionale, che ha precisato come posta elettronica e messaggi inviati tramite l'applicazione WhatsApp rientrano a pieno titolo nella sfera di protezione dell'art. 15 Cost., apparendo del tutto assimilabili a lettere o biglietti chiusi, ma riferendosi esclusivamente ad account personali.

Gli *account* con dominio aziendale e/o dell'ente (siano essi generici o personalizzati), acquistati e decisi dal datore di lavoro, in quanto strumenti di lavoro devono essere oggetto di controllo e/o utilizzo datoriale e spesso debbono rispettare obblighi di conservazione decennali o anche ulteriori se di rilevanza pubblica. In presenza di detti obblighi di conservazione, si osserva come la raccolta dei metadati sarebbe sempre "imposta" da obblighi di legge.

I principi di lecito trattamento dei dati personali contenuti nei messaggi e nei metadati della posta elettronica affidata dal datore di lavoro

L'impiego di qualunque strumento di lavoro informatico/informativo, inclusi programmi e servizi di gestione degli *account* di posta elettronica aziendale e/o dell'ente, implica "trattamenti" di dati personali riferiti a "interessati" identificati o identificabili nel contesto lavorativo (art.4, par.1, n.1 e 2 GDPR). Sicché il datore di lavoro in qualità di titolare del trattamento è sempre tenuto a rispettare i principi generali di trattamento (artt.5, 24 e 25 GDPR) e a fornire a qualunque interessato nel contesto lavorativo

AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

(dipendente/collaboratore) una adeguata informativa sul complessivo trattamento effettuato delle informazioni personali (art.13 e 14 GDPR).

Quanto alla sussistenza di idonei presupposto di liceità (art.5 par.1 lett.a) GDPR art.6 e art.9 GDPR), le basi giuridiche del trattamento dei dati personali nel contesto lavorativo e/o di collaborazione per i dati comuni sono quelle contenute nell'art.6 lett. b), c) d) f) GDPR (per le pubbliche amministrazioni anche nell'art.6 par.1 lett. e) GDPR), mentre per i dati particolari sono contenute nell'art.9 par. 2 lett. b), c) d) e) f) h) GDPR (per le pubbliche amministrazioni anche nell'art.6 par.1 lett.e) GDPR).

Vero è che grava sul datore di lavoro privato e/o pubblico, in attuazione del principio di responsabilizzazione (art.5 par.2 e art.24 GDPR), 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 (*Data Protection Impact Assessment* artt.35 e 36 GDPR). Tuttavia si manifesta preoccupazione per l'estensione dell'esigenza di procedere con una valutazione d'impatto in caso di introduzione di *account* aziendali e/o dell'ente per lo svolgimento del rapporto di lavoro. Gli 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) sono tutte informazioni connesse allo svolgimento dell'attività lavorativa e non certo informazioni riservate e segrete del lavoratore.

Simile lettura del Regolamento GDPR svilisce l'esigenza che la valutazione d'impatto sulla protezione dei dati debba essere effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche (art.35 par.1 GDPR) e rischia di condurre ad un aggravio di costi indipendentemente dalla reale esistenza di elevati rischi per i diritti e le libertà delle persone.

Ritenere sempre obbligatoria una DPIA in caso di uso di nuove tecnologie e/o utilizzo di *account* di posta elettronica potrebbe avere come effetto quello di svilire l'obbligo in esame poiché implica una svalutazione del fatto che il presupposto cruciale per la valutazione di impatto (art.35 GDPR) è connesso all'esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Del resto questa era l'impostazione prescelta dall'Autorità Garante nell'Allegato 1 al Provvedimento n.467 11 ottobre 2018 (doc. web n. 9058979 Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018). L'indicazione dell'Autorità Garante Italiana di ritenere che comunque, in caso di utilizzo di *account* di posta elettronica aziendale e contestuale raccolta di metadati, debba essere sempre effettuata una valutazione di impatto stante la "vulnerabilità" degli interessati e il rischio di "monitoraggio sistematico" rischia di imporre un pesante e ingiustificato aggravio per le PMI e gli enti pubblici.

L'applicazione delle previsioni italiane di maggior tutela per i lavoratori dipendenti in occasione del trattamento dei dati personali

Quanto al contesto normativo tutto italiano, esistono previsioni normative che prescrivono condizioni più specifiche per assicurare la protezione dei dati personali ai sensi dell'art.88 par.1 GDPR. L'art.4 e l'art.8 legge n.300/1970 prescrivono specifiche tutele che interessano solo e soltanto i dipendenti e non anche coloro che prestano a vario titolo attività lavorativa all'interno delle organizzazioni.

AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

La riscrittura dell'art.4 legge n.300/1970 nel 2015 per effetto del *Jobs Act* ha aggiornato la norma consentendo l'utilizzo di strumenti di lavoro preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla "registrazione degli accessi e delle presenze" e allo "svolgimento della prestazione".

Il Comunicato del Ministero del Lavoro 18/06/2015, pubblicato a seguito della modifica dell'art. 4 legge n. 300/1970, precisa quanto segue: "La modifica all'articolo 4 dello Statuto chiarisce, poi, che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" (una volta si sarebbero chiamati gli "attrezzi di lavoro"), come pc, tablet e cellulari. In tal modo, viene fugato ogni dubbio - per quanto teorico- circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti.

L'espressione "per rendere la prestazione lavorativa" comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi *software* di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione. Perciò, è bene ribadirlo, non si autorizza nessun controllo a distanza; piuttosto, si chiariscono solo le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti."

Per quanto di interesse la Circolare dell'Ispettorato Nazionale del Lavoro n. 2/2016, fornendo indicazioni operative ai sensi dell'art. 4, commi 1 e 2, l. n. 300/1970 sull'utilizzazione di impianti GPS sostiene come: "... l'interpretazione letterale del disposto normativo (n.d.r. art.4 l.n.300/1970) porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità sia stati posti in uso e messi a sua disposizione. In linea di massima, e in termini generali, si può ritenere che i sistemi di sistemi di geolocalizzazione rappresentino un elemento "aggiunto" rispetto agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro. Pertanto gli impianti di GPS per poter essere legittimamente utilizzati debbono essere autorizzati dall'Ispettorato o dalla contrattazione collettiva (art.4 comma 1, l. n.300/1970).

L'adozione di *account* di posta elettronica aziendali e/o dell'ente implica l'affidamento al dipendente di uno "strumento di lavoro" necessario allo svolgimento della prestazione, il cui funzionamento soggiace agli obblighi di trasparenza e di una specifica informativa ex art. 4, comma 1, l. n. 300/1970. Gli *account* di posta elettronica forniti dal datore di lavoro sono sempre strumenti di lavoro ex art.4 comma 2 l.n.300/1970 e i metadati (raccolti dai *provider* di posta) contengono informazioni personali del lavoratore attinenti all'esecuzione della prestazione e quindi sempre rilevanti ai fini del rapporto di lavoro e della eventuale valutazione dell'idoneità professionale *ex* art.8 legge n.300/1970.

Escludere che l'*account* di posta elettronica aziendale e/o dell'ente sia uno strumento di lavoro induce poi l'Autorità Garante a ritenere che l'eventuale raccolta dei metadati per oltre 7 giorni sia un'attività di controllo a distanza dell'attività lavorativa. Simile interpretazione rischia di vanificare l'aggiornamento di

AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

una norma come l'art.4 legge n.300/1970 previsto dal d. lgs. n. 151/2015 che, in attuazione di quanto specificamente previsto dalla legge delega n.183/2014, è intervenuta proprio per consentire l'utilizzo di strumenti di lavoro senza l'esigenza di sottoscrivere accordi sindacali/ricevere preventiva autorizzazione dell'Ispettorato Territoriale del Lavoro.

Parrebbe inoltre che l'Autorità Garante non tenga in adeguato conto la differenza tra la conservazione dei metadati e il controllo sui medesimi relativamente alla posta elettronica da parte dei dipendenti; conservare (anche) i metadati non implica automaticamente un controllo sull'attività lavorativa o addirittura l'acquisizione di informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

In ogni caso pare importante evidenziare come la conservazione dei metadati oltre 7 giorni potrebbe rispondere altresì a legittimi interessi e diritti dei dipendenti. La repentina cancellazione di informazioni essenziali delle *mail* potrebbe ledere l'esercizio del diritto di difesa privando il dipendente della possibilità di dimostrare la propria estraneità a fatti di cui fosse ingiustamente accusato.

Si osserva ancora come secondo il ragionamento dell'Autorità Garante dovrebbe essere oggetto di accordo sindacale/autorizzazione lo stesso utilizzo di software che registrino l'attività quotidiana di ciascun operatore (es. Microsoft 365) con un irragionevole aggravio burocratico e di costi per le PMI e gli enti pubblici impossibilitate a sottoscrivere accordi sindacali per l'assenza di rappresentanze nelle realtà di ridotte dimensioni con meno di quindici dipendenti. Per non parlare poi dell'aggravio a cui sarebbero onerati gli uffici dell'Ispettorato del Lavoro qualora dovessero procedere ad autorizzare la conservazione dei metadati degli account aziendali e/o dell'ente se superiore a 7 giorni.

Da ultimo l'Autorità Garante non considera che la raccolta dei "metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica e relativi alle operazioni di invio, ricezione, e smistamento dei messaggi di posta elettronica (che possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei PC coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione e di ricezione, la dimensione del messaggio, la presenza e la dimensione degli eventuali allegati, in certi casi anche l'oggetto del messaggio spedito o ricevuto)" viene effettuata dal provider ed è strettamente connessa all'esigenza di fornire un servizio all'azienda e/o all'ente utilizzatore degli *account* di posta. Si tratterebbe insomma di una raccolta effettuata dal provider e non dal datore di lavoro, strettamente connessa ai programmi e servizi informatici di gestione della posta elettronica, la cui limitazione potrebbe compromettere il servizio stesso precludendo al datore di lavoro di disporre degli elementi indispensabili per poter comprovare e documentare invio/ricezione delle comunicazioni telematiche con conseguente grave lesione della possibilità di tutelare i propri diritti.

La conservazione dei metadati come strumento di "igiene" informatica

Pare opportuno da ultimo considerare altresì che la conservazione dei metadati degli *account* aziendali/dell'ente potrebbero essere considerato come uno strumento di protezione informatica minimo e rientrare tra le misure di "igiene" informatica codificate per le PMI in occasione del recepimento della direttiva UE n.2023/2555 (cd. NIS II)[2]. Secondo le prime indicazioni della Commissione europea le

[2] Cfr. C. Ogriseg, *Network and Information Security: la strategia europea nella Direttiva NIS II e le sfide che ci attendono* in *Ciberspazio e diritto*, vol. 25, n. 76 (1 - 2024), pp. 131-148.

AVV. CLAUDIA OGRISEG *
AVV. ALBERTO TARLAO

VIA CARDUCCI 44 – UDINE 33100
T +39 0432 512704 F +39 0432 503901

misure di gestione dei rischi di sicurezza informatica, da codificarsi in ciascuno Stato entro giugno 2024, dovranno proteggere non solo i sistemi informativi e di rete, ma anche l'ambiente fisico da eventi (quali sabotaggi, furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente) o da qualsiasi accesso fisico non autorizzato (in grado di compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi).

In un contesto di rafforzamento dei requisiti di sicurezza informatica l'attenzione da dedicare alle misure di *risk management* (alla *governance*, ai rischi di *cybersecurity*, alle misure di *management*, al *multi-risk assessment* della filiera), imporrà nuovi decaloghi di *accountability* in tema di *cyber* sicurezza secondo un approccio multi-rischio. Nell'ambito di una razionalizzazione degli obblighi di reportistica e notifica, unitamente alla promozione dell'uso di schemi europei di certificazione volontaria attinenti alla *cybersecurity*, la conservazione dei metadati delle *mail* per un tempo superiore a 7 giorni potrebbe ragionevolmente essere considerata misura di "igiene" di sicurezza. Una misura minima, indispensabile, da adottare sempre in presenza dell'uso di *account* aziendali, non certo discrezionale e compatibile con l'esigenza di ottenere una preventiva autorizzazione dell'Ispettorato o un accordo sindacale per poter essere adottata.

****

Per tutte le ragioni sopra esposte si confida che l'Autorità Garante Italiana possa rivalutare l'opportunità di considerare l'utilizzo di *account* di posta elettronica con conservazione dei metadati oltre 7 giorni sempre come una *attività di controllo a distanza* soggetta alle garanzie dell'art.4 comma 1 l. n.300/1970 ossia la preventiva sottoscrizione di un accordo sindacale o l'autorizzazione dell'Ispettorato del Lavoro.

Udine 15 aprile 2024

avv. Claudia Ogriseg
avv. Alberto Tarlao