La Privacy e l’email del dipendente: il punto della situazione

scritto da goal | 16 Marzo 2020

di Stefano Bacchiocchi*

Dopo quasi due anni dall’introduzione del nuovo regolamento privacy (GDPR, 25/05/2018), con la newsletter n. 460 del 20 dicembre 2019 il Garante privacy è tornato a fornire alcune importanti indicazioni circa le email aziendali in uso ai dipendenti. Poiché ormai l’uso delle email aziendali è all’ordine del giorno di qualsiasi ufficio professionale, credo sia giusto fare il punto della situazione con un taglio pratico. Fornire linee guida in questo campo non è semplice, poiché è necessario bilanciare le legittime pretese del datore di lavoro e quelle, altrettanto legittime, dei dipendenti e collaboratori. Le risposte sono da cercare attraverso il coordinamento e l’interpretazione di molte norme, di diverso rango e fonte. La prima norma è sicuramente lo Statuto dei lavoratori (legge 20 maggio 1970, n. 300), che all’articolo 4 pone i principi ed i limiti affinché il controllo del dipendente da parte del datore di lavoro possa dirsi legittimo. Pertanto, in linea di massima, è ammissibile che si possa controllare il dipendente “per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale”, salvo gli accordi o autorizzazioni previsti *ex lege*. Tuttavia, anche se ci fossero questi accordi/ autorizzazioni, il datore di lavoro non può accedere ai dispositivi aziendali concessi in dotazione ai lavoratori per meri scopi “investigativi”. L’articolo 4 citato prosegue specificando che “Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d’uso degli strumenti e di

effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196". Ecco qui il primo vero ed esplicito intreccio tra controllo e privacy: è fatto obbligo al datore di lavoro di dotarsi di una politica aziendale che sia esplicita e nota ai dipendenti. Se, per esempio, un licenziamento disciplinare fosse basato su illeciti rinvenuti nelle email del dipendente, il provvedimento rischierebbe concretamente di essere viziato ed annullato qualora sia stato attivato in mancanza di legittimità delle policy aziendali. Questo è perfettamente in linea con quanto previsto sia dal GDPR sia dalle indicazioni del Garante della privacy: solo la sottoscrizione di un'informativa privacy ex art 13 GDPR (e della corretta policy aziendale) da parte del lavoratore, legittima il datore di lavoro (titolare del trattamento) a prendere visione delle email pervenute nella posta elettronica aziendale. Spesso si crede, erroneamente, che la semplice lettura della email dei dipendenti non comporti alcun problema di privacy. Accade sovente che il datore di lavoro pensi che, avendo la proprietà del mezzo (server di posta, personal computer, ecc.), sia legittimo accedere senza particolari formalità alle email aziendali in uso ai dipendenti. Nulla di più errato; quando c'è un rischio privacy il datore di lavoro deve intervenire, per legge, a sua tutela. Ma quando è imperativo intervenire? Basta citare il Considerando 75 del GDPR che descrive il concetto di rischio in tema privacy: "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, …, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li

riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati". L'email aziendale è sicuramente un mezzo che può veicolare i trattamenti descritti nel citato Considerando 75 al GDPR. Da qui l'obbligo di intervenire. Quando è opportuno far sottoscrivere l'informativa e la policy aziendale? Il momento migliore è certamente alla conclusione del contratto di lavoro. Se ci fossero delle modifiche in corso d'opera, è imperativo fornire le modifiche e/o integrazioni al dipendente tempestivamente e per iscritto. Poiché spesso queste modifiche sono frutto di un cambiamento in ordine alle procedure informatiche e/o cambio di software/ hardware, è opportuno coordinarsi tempestivamente con il proprio responsabile dei sistemi e con il DPO (se nominato). È un momento delicato e (in ottica di consulenza ai nostri clienti) sarebbe opportuno coinvolgere anche le rappresentanze sindacali, se del caso. Cosa fare quando un dipendente cessa il rapporto lavorativo (dimissioni, licenziamenti, ecc.)? È certamente un illecito del datore di lavoro mantenere attivo l'account di posta aziendale di un dipendente dopo l'interruzione del rapporto di lavoro ed accedere alle mail contenute nella sua casella di posta elettronica. È lo stesso garante privacy che nella newsletter n. 460 del 20 dicembre 2019 specifica (come era prevedibile) che "la protezione della vita privata si estende anche all'ambito

lavorativo". Non è lecito, infatti, che i datori di lavoro abbiano accesso alle comunicazioni pervenute nella email aziendale del lavoratore, anche dopo che questi abbia cessato il suo rapporto di lavoro subordinato. Il Garante continua: "subito dopo la cessazione del rapporto di lavoro, un'azienda deve infatti rimuovere gli account di posta elettronica riconducibili a un dipendente, adottare sistemi automatici con indirizzi alternativi a chi contatta la casella di posta e introdurre accorgimenti tecnici per impedire la visualizzazione dei messaggi in arrivo". Non dimentichiamoci che anche il semplice scambio di email con altri dipendenti potrebbe portare a conoscere informazioni personali relative al lavoratore; persino non aprire i messaggi permette di ricavare dati importanti quali: data, ora oggetto, nominativi di mittenti e destinatari, ecc. È opportuno, inoltre, che il datore di lavoro si affretti (in ottica di *accountability* ed, eventualmente, per obbligo di legge), qualora non sia già stato fatto, alla redazione della c.d. DPIA (Data Protection Impact Assessment). La citata valutazione di impatto è un documento fondamentale che deve essere predisposto dal titolare del trattamento stesso. In buona sostanza, si tratta di una valutazione preventiva (prima di iniziare il trattamento) delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. In ogni caso, il titolare del trattamento dovrà motivare le sue valutazioni e redigere il registro dei trattamenti (obbligatorio).

Il titolare, quando svolge la valutazione di impatto, deve poi consultarsi col DPO (se nominato) il quale ha il compito di fornire un parere formale in merito alla valutazione di impatto e sorvegliarne lo svolgimento. In sintesi, è opportuno:

- che venga preparata e sottoscritta dai dipendenti una dettagliata policy aziendale (concordata anche con le rappresentanze sindacali, se la situazione lo richiede);
- predisporre e far sottoscrivere una informativa privacy

ex art.13 GDPR;

- coordinare le operazioni di aggiornamento e modifiche con i responsabili dei sistemi, col DPO (se nominato) e se del caso con le rappresentanze;
- se si opera in settori con alti volumi di dati, elevato numero di dipendenti e/o particolari categorie di dati (es. sanitari, giudiziari, ecc.), predisporre una DPIA (analisi e valutazione del rischio privacy) adeguata;
- inserire la gestione delle email, se del caso, nel registro dei trattamenti obbligatorio.

* *Odcec Brescia*