

Conservazione delle e-mail aziendali. E' necessaria un'adeguata informativa per evitare sanzioni

Luca Failla - Professore a contratto di Diritto del Lavoro presso l'Università degli Studi LUM

Per la salvaguardia della propria attività, le aziende possono prevedere un sistema di raccolta, gestione e conservazione dei dati, anche delle mail, che tuteli dipendenti e collaboratori accompagnato da un'adeguata informativa sull'uso degli strumenti aziendali e di lavoro. E' fondamentale, però, che le aziende facciano un costante monitoraggio delle informative e una valutazione periodica di un loro aggiornamento con attenzione al contenuto ed alle finalità dichiarate del trattamento dei dati: sempre più oggi, nel contesto in continua evoluzione delle conoscenze tecniche, degli orientamenti del Garante della Privacy e della legislazione speciale che interviene periodicamente in questa materia, un elemento dal quale non è possibile prescindere. Attenzione: perché pare accentuarsi il divario preoccupante fra prassi abitualmente ritenute lecite delle aziende e sanzioni ex post di quelle stesse prassi da parte del Garante della Privacy.

Con provvedimento n. 472 del 17 luglio 2024, il **Garante della privacy** ha (pesantemente) **sanzionato** una società per ritenuta violazione delle disposizioni del GDPR (Regolamento n. 679/2016) ed, in particolare, per comportamenti riconducibili ad un'**illecita raccolta, trattamento e conservazione** (art. 5, par. 1 lett. a), c) ed e) relative rispettivamente ai principi di liceità, adeguatezza e limitazione del trattamento) delle **mail aziendali** di un proprio ex agente di commercio scambiate nel corso del rapporto di collaborazione, da cui poi l'azienda aveva tratto elementi ed informazioni per avviare a danno dello stesso un giudizio per concorrenza sleale ex art. 2598 n. 3 c.c.

Al di là del merito della vicenda scaturita da un esposto, quale reazione dell'ex collaboratore all'azione di concorrenza sleale intentatagli dalla società, a seguito di quanto emerso dal controllo delle mail aziendali successivamente alla cessazione del rapporto, quello che stupisce nel caso concreto è la **gravità** con cui il **Garante della privacy** ha **valutato** nel suo complesso il **comportamento** dell'azienda dal **punto di vista tecnico**, irrogando una sanzione di ben euro 80.000 ed inibendo il trattamento e la conservazione delle mail. Ordine questo che certamente avrà un **impatto** anche nel **giudizio di concorrenza sleale** nel frattempo avviato ai danni dell'ex agente. Quello **sanzionato** sarebbe stato, infatti, l'uso di un **dispositivo MailStore** (peraltro utilizzato da un gran numero di aziende) che garantiva il **back-up** delle **caselle di posta elettronica di tutti i dipendenti**, ivi compreso l'ex agente.

Si legge, infatti, nel provvedimento "risulta che attraverso tale dispositivo la società effettua il backup del contenuto delle caselle di posta elettronica in uso ai dipendenti e ai collaboratori, in vigenza del rapporto di lavoro/collaborazione, conservandone il contenuto in modo sistematico e automatico per un periodo di tempo pari a tre anni, dopo la cessazione dei rapporti lavorativi. La società ha dichiarato, nelle memorie difensive, che la finalità di tale trattamento è garantire la sicurezza dei sistemi informatici, ai sensi dell'art. 5, par. 1, lett. f), del Regolamento". Peraltro, l'**eventualità di conservazione delle e-mail** aveva formato adeguatamente **oggetto dell'informativa** ex art. 13 GDPR **consegnata al collaboratore**.

A ciò si aggiunga che il Garante ha altresì ritenuto la **mail aziendale** (ed il successivo back up effettuato tramite MailStore) **integrante un controllo aziendale a distanza** ex art. 4 della legge n. 300/1970 che avrebbe richiesto l'adozione di un accordo aziendale previsto dalla stessa norma. Il che pare francamente eccessivo, considerato che lo stesso art. 4 esenta dall'adozione della procedura autorizzativa sindacale o amministrativa gli strumenti di lavoro, come

certamente la posta aziendale, e di conseguenza il back up della stessa.

Leggi anche dello stesso Autore:

[Gestione delle e-mail: cosa possono fare le aziende in attesa di altre \(opportune\) determinazioni del Garante della Privacy?](#)

Criticamente deve essere osservato che la **cessazione del rapporto professionale** se da un lato comporta - come precisato anche dal Garante della privacy con il provvedimento n. 216/2019 - la chiusura dell'account del dipendente e del collaboratore, la stessa **non può contemplare obbligatoriamente** a carico delle aziende la **cancellazione immediata** anche dei **dati di back-up** per due ordini di ragioni molto semplici:

- la prima è che i dati di back-up sono solitamente aggregati e vengono separati ed acquisiti solo in caso di necessità (come, ad esempio, l'acquisizione di elementi di prova necessari per il contenzioso, nel caso di specie peraltro incredibilmente escluso dal Garante sul presupposto - si intuisce - che precontenzioso possa sussistere solo se l'azienda debba difendersi da una azione esterna e non promuoverla come invece lecitamente nel caso di specie);

- la seconda, ben più rilevante, è che la previsione della possibilità di una conservazione dei dati/mail aziendali - se oggetto di adeguata informativa anche nei confronti dei collaboratori - è lecito principio di gestione dei dati, contemplato dal Regolamento e riconosciuto legittimo anche per ragioni di sicurezza informatica. Purché contenuto entro tempi ragionevoli quali ad esempio i tre anni previsti nel caso specifico, i quali non paiono un periodo eccessivamente dilatato.

La difesa della società, peraltro, lo aveva evidenziato correttamente laddove veniva indicato come il **back up sulle caselle e-mail**, eseguito mediante l'applicativo contestato, fosse "una **misura tecnica di sicurezza**" disposta in ottemperanza all'art. 5, par. 1, lett. f) del Regolamento "per garantire la sicurezza e l'integrità dei dati personali trattati da attacchi informatici (...). L'esecuzione del backup non richiede alcun accesso da parte del personale aziendale, mentre il periodo massimo di conservazione pari a tre anni è un parametro teorico che delimita il tempo massimo di retention e, di conseguenza, il tempo massimo per cui è possibile recuperare dati e/o informazioni a ritroso in caso di disservizio o attacco informatico".

Forse quello che **era mancato** nell'**informativa aziendale** era che il **back up delle mail** oltre che a tutela dell'integrità aziendale a **protezione** da eventuali **attacchi informatici**, fosse altresì **finalizzato** alla **tutela del patrimonio** e del **know how aziendale** (informazione che avrebbe portato l'agente infedele a cancellare tempestivamente le mail in questione integranti la violazione dell'obbligo di fedeltà, come poi invece scoperto dall'azienda).

Ed il punto è proprio questo. Il Garante della Privacy ha **posto l'accento** su **attività** che rientrano nella **legittima gestione** delle **attività d'impresa**.

È, infatti, normale che per la salvaguardia della propria attività, le aziende prevedano un **sistema di raccolta, gestione e conservazione dei dati**, senza per questo pregiudicare la posizione di **dipendenti e collaboratori**, tutelati attraverso un'**adeguata informativa** sull'uso degli strumenti aziendali e degli strumenti di lavoro. Perché non dimentichiamo che la **casella di posta elettronica** è pur sempre uno **strumento di lavoro**, e ciò diversamente - va ribadito - da quanto anche con tale provvedimento il Garante continua a sostenere, per il quale infatti sarebbe **richiesto l'accordo aziendale** ex art. 4 della legge n. 300/1970. Accordo che nessuna azienda si sogna di negoziare con le organizzazioni sindacali, che infatti neppure lo pretendono.

A maggior ragione lo è la **casella di posta aperta** - per ragioni aziendali - a favore di un agente di commercio - che è un lavoratore autonomo - per facilitare le relazioni commerciali con la clientela (che è pur sempre dell'azienda). Per tale ragione, appaiono altresì ultronee le osservazioni del Garante in merito all'obbligo di attivare la procedura di autorizzazione preventiva per l'uso del software deputato alle attività di back-up e conservazioni dei dati. Proprio perché la casella di posta è pur sempre solo uno strumento di lavoro aziendale il cui uso non può rientrare - come già detto - nelle previsioni obbligatorie dell'art. 4, comma 1, della legge n. 300/1970.

Peraltro, in tema di **conservazione dei metadati** delle caselle di posta elettronica, con provvedimento del Garante della privacy 21 dicembre 2023, n. 642, poi **rettificato** (in chiave, peraltro, di **“raccomandazione”** e non di “prescrizione”) dallo stesso Garante lo scorso 6 giugno 2024, erano emerse da subito **due importanti novità**:

- una più precisa indicazione di **cosa si intende per “metadati”** ossia solo quelli registrati automaticamente dai sistemi di posta elettronica: “tecnicamente le 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)”;

- il **carattere meno precettivo del provvedimento** che, proprio perché è un **documento di indirizzo** non può - si legge nell’introduzione - “recare prescrizioni, nè introduce nuovi adempimenti a carico dei titolari del trattamento ma intende offrire una ricostruzione sistematica delle disposizioni applicabili (...) 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”.

È chiaro come uno di questi **punti di attenzione** sia proprio l’**adeguatezza dell’informativa** a supportare l’uso di strumenti tecnici di raccolta e conservazione dei dati, ivi compresi i programmi che svolgano una funzione di back up analoga a quella segnalata, per finalità anche di tutela del patrimonio e del know how aziendale (a giudizio del Garante mancante nel caso in esame). Ma se la **conservazione per 21 giorni**, oggi consigliata dal Garante, si configura nel contesto del nuovo provvedimento come un **“minimo” ragionevole**, visto che è indicata “a titolo orientativo”, non è certamente possibile ritenere un termine di tre anni dalla cessazione del rapporto del tutto irragionevole, come invece ritenuto dal Garante, specie se la finalità, come già detto, è, non quella di controllare dipendenti e collaboratori, ma unicamente quella della tutela dell’attività e dei dati aziendali.

Al di là del caso concreto, su cui certamente il provvedimento in esame, se non impugnato, determinerà conseguenze significative anche sul giudizio per concorrenza sleale intentato a danno dell’ex agente - vista l’impossibilità di utilizzare i dati/mail dell’agente integranti l’illiceità della condotta - il **costante monitoraggio delle informative aziendali** - questo sì - e la valutazione periodica di un loro **aggiornamento** e di una loro **implementazione** con un’attenzione al contenuto ed alle finalità dichiarate del **trattamento dei dati acquisiti dei dipendenti e collaboratori**, sono sempre più oggi, nel contesto in continua evoluzione delle conoscenze tecniche, degli orientamenti del Garante e della legislazione speciale che interviene periodicamente in questa materia, un elemento fondamentale di **corretta gestione dell’attività dell’impresa**, dal quale non è possibile prescindere.

Nella sostanza invece, pare **accentuarsi il divario** preoccupante fra **prassi abitualmente ritenute lecite delle aziende** e **sanzioni ex post** di quelle **stesse prassi** da parte del **Garante della Privacy**.