PROVACY

Accesso alle mail dei dipendenti: come farlo nel pieno rispetto delle leggi e dei diritti

L'accesso del datore di lavoro alle mail dei dipendenti è regolato da normative complesse e richiede attenzione per evitare violazioni della privacy. Ecco le linee guida, le sentenze rilevanti e i consigli pratici per stabilire regole interne che garantiscano la conformità legale e proteggano la dignità e la riservatezza dei lavoratori

Pubblicato il 14 ott 2024

Marco Catalano
Avvocato, Consulente privacy

Alfredo Zallone
Avvocato, Consulente privacy

Quando si parla di accesso da parte del datore di lavoro alle e-mail del dipendente, bisogna essere consapevoli che si entra in un campo minato.

Proprio perché l'argomento è molto complesso (lungi dal volere in questa sede fare un trattato sulla tematica) è bene conoscere la materia, imparare e studiare le diverse normative che si intrecciano, e regolamentarla internamente per determinare gli eventuali accessi alle e-mail siano a rischio "mine".

Sicuramente è un tema, questo, che per aziende con centinaia o migliaia di dipendenti può risultare ad alto rischio, ma ciò non deve indurre il lettore al pensiero che un'azienda con un numero limitatissimo di dipendenti possa essere indifferente alla materia, ricordando invece che anche in "aree" a basso rischio, si possono nascondere "ordigni pericolosi".

Pertanto, è bene prima di tutto definire le regole necessarie e portarle a conoscenza di tutto il personale, senza dimenticare di istruire le persone deputate all'applicazione delle stesse all'interno dell'azienda.

Capisaldi questi che sicuramente contribuiscono ad una maggiore sensibilizzazione sul tema, riducono i rischi di non conformità e quindi, seguendo la nostra metafora, "evitano di fare feriti". In particolare, occorre fare in modo che il personale deputato sia messo nelle condizioni di poter esaminare la situazione, capirne i rischi (se – effettivamente – ve ne siano) e fermarsi in tempo davanti ad una "mina inesplosa" chiedendo supporto al personale qualificato per capire come procedere.

Indice degli argomenti

Le regole nel contesto nazionale

Come abbiamo detto, sono diverse le regole da tenere in considerazione quando il datore di lavoro decide di accedere alle e-mail del dipendente: vi sono norme da rispettare, gli orientamenti giurisprudenziali della Corte di Cassazione da tenere in considerazione oltreché i provvedimenti emessi dall'Autorità Garante per la Protezione dei Dati Personali (di seguito anche "**Garante**").

Le Linee guida del Garante

In merito alle e-mail del dipendente, è bene ricordare che già le **Linee guida del Garante per posta elettronica e internet (doc. web. 1387522) del marzo 2007**, in materia di posta elettronica, prevedono che "**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**, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un ´ulteriore protezione deriva dalle norme penali a tutela dell´inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale)".

Considerazione questa, ancora perfettamente attuale nell'interpretazione del Garante, al punto che trovarne conferma risulta molto semplice: basti pensare al provvedimento n. 53 del 1° febbraio 2018 del Garante (doc. web n. 8159221) "Inoltre **il datore di lavoro**, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, **deve in ogni caso salvaguardarne la libertà e la dignità** […]" oppure, senza andare troppo indietro, al provvedimento n. 364 del 6 giugno 2024 in ambito di "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", in cui viene richiamato il seguente principio: "[…] Ciò comporta che, **anche nel contesto lavorativo pubblico e privato, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza** […]".

Dello stesso avviso appare la Corte di Cassazione, "([…] si veda in proposito Cass. 31.3.2016, n. 13057, laddove si afferma che qualora **"siano attivate caselle di posta elettronica – protette da password personalizzate – a nome di uno specifico dipendente, quelle «caselle» rappresentano il domicilio informatico proprio del dipendente** […]. **La casella rappresenta uno «spazio» a disposizione – in via esclusiva – della persona, sicché la sua invasione costituisce, al contempo, lesione della riservatezza**"). […]." oppure la Cassazione civile, Sez. lavoro, Sent. n. 25732 del 22.09.2021 che, in ambito di controlli sul lavoratore, afferma: "[…] Innanzitutto, va riaffermato il principio, già richiamato, espresso dalla giurisprudenza di questa Corte formatasi nel vigore della precedente formulazione dell'art. 4 dello Statuto dei lavoratori, secondo cui **in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore** (Cass. n. 15892 del 2007, cit.; Cass. n. 4375 del 2010, cit.; Cass. n. 16622 del 2012, cit.; Cass. n. 9904 del 2016; Cass. n. 18302 del 2016, cit.).

Inoltre, proprio per cercare di porre rimedio a questo confine "labile" dell'accesso alle email da parte del datore di lavoro, già il "WP 55 – Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro – adottato il 29 maggio 2002" del WP29, come anche le Linee Guida del 2007, sopra citate, suggerivano al datore di lavoro di valutare "**la**

possibilità di attribuire al lavoratori un diverso indirizzo destinato ad uso privato del lavoratore" in quanto "[…] consentire ai dipendenti l'impiego di un indirizzo privato o di webmail, potrebbe contribuire a risolvere in modo pragmatico il problema in questione. **Una raccomandazione del datore di lavoro in tal senso chiarirebbe la distinzione tra messaggi di posta elettronica destinati ad uso professionale e quelli con finalità private e ridurrebbe la possibilità che i datori di lavoro invadano la sfera privata dei loro dipendenti**." […] "Una tale politica può inoltre **risultare vantaggiosa per i dipendenti poiché darebbe loro la certezza del livello di rispetto della sfera privata che possono attendersi**, certezza che può essere assente in codici di condotta più complessi e confusi".

Premesso quindi che la e-mail del lavoratore, secondo l'interpretazione consolidata del Garante, rientra nella sfera di protezione della vita privata del lavoratore, **è bene che il datore di lavoro tenga a mente che non può avere mano libera** o possa accedere indiscriminatamente alle e-mail del dipendente, per di più se tale accesso avvenga per porre in essere controlli sul lavoratore interessato.

L'art. 4 dello Statuto dei lavoratori

Sul punto, infatti, appare fondamentale richiamare l'art. 4 della Legge n. 300/1970 (anche "Statuto dei Lavoratori"), in materia di "impianti audiovisivi e strumenti di controllo" che definisce come gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, dunque al di fuori dell'ambito di applicazione del comma 2 del menzionato articolo, possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali; inoltre le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, solo previa comunicazione ai lavoratori delle modalità d'uso di tali strumenti e della effettuazione dei controlli "e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

L'art. 114 del Codice Privacy

In tal senso oltre al rispetto – in linea generale – delle norme in materia di protezione dei dati personali, si ricorda che il Legislatore nazionale ha sempre voluto attribuire molta importanza a tale disposizione, dedicando un articolo specifico del Codice Privacy: **Art. 114 (Garanzie in materia di controllo a distanza).** "1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300."

Privacy e diritto del lavoro, infatti, sono uniti da un filo comune.

Le finalità per le quali il datore di lavoro decide di accedere alle mail del dipendente

Innanzitutto, così come per un campo minato, la prima questione è comprendere quali siano finalità per le quali il datore di lavoro decide di accedere alle e-mail del dipendente.

Si badi bene: **i motivi di accesso alla e-mail del dipendente possono essere svariati e non sono a priori illeciti o in violazione della normativa**, è tuttavia necessario indagare quali essi siano. Si può fare una elencazione esemplificativa che vada dai casi più "gestibili" ai più "scomodi": il datore di lavoro potrebbe avere la necessità di accedere alla e-mail del lavoratore in caso di assenza non programmata, improvvisa o prolungata del lavoratore (l'esempio è alla malattia) oppure per improrogabili necessità legate all'attività lavorativa ma anche per difendersi in giudizio oppure per accertare specificamente condotte illecite del dipendente.

Altro elemento rilevante è il tempo: l'accesso alla e-mail del lavoratore può avvenire in costanza di rapporto lavorativo oppure in seguito alla cessazione del rapporto, anche dopo un licenziamento.

In tutti questi casi, **l'interesse del Titolare ad accedere** alle informazioni necessarie all'efficiente gestione della propria attività deve essere sempre contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte del dipendente (o ex-dipendente).

La corretta base giuridica del trattamento

È sempre opportuno che il datore di lavoro verifichi **la liceità dell'accesso alle e-mail, valutando la corretta base giuridica del trattamento** e "[…] 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)."

In merito a ciò, nel **provvedimento n. 8 dell'11 gennaio 2023** del Garante, l'Autorità specifica come "[…] il legittimo interesse a trattare dati personali per difendere un proprio diritto in giudizio non possa comportare un **aprioristico annullamento del diritto alla protezione dei dati personali riconosciuto agli interessati** considerato, tra l'altro, che 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, […]".

Va da sé che ogni qualvolta il datore di lavoro decida di accedere alle e-mail del lavoratore, è imprescindibile che effettui le opportune valutazioni per comprendere se l'area attenzionata sia una

zona a basso rischio o un “campo minato”, soprattutto se l’accesso alle e-mail avviene per effettuare controlli.

I controlli

I controlli e, quindi l’accesso alla e-mail del lavoratore, devono avvenire nel pieno rispetto dell’art. 4 dello Statuto dei Lavoratori e dei principi del trattamento di dati personali previsti dall’art. 5 del Reg. (UE) 2016/679 (di seguito il “Regolamento”).

In questi casi, pertanto, **l’azienda ricopre due vesti**: datore di lavoro del dipendente e titolare del trattamento dei dati personali dell’interessato. Da questo duplice ruolo deriva uno sdoppiamento degli obblighi in carico a tale soggetto.

Infatti, il titolare del trattamento è tenuto a rispettare i principi generali del trattamento (in particolare, gli 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 (tra i quali si vedano gli 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 consapevoli, prima che il trattamento abbia inizio, delle caratteristiche dello stesso. Tale consapevolezza si può realizzare solo se al dipendente sono state fornite sia una idonea informativa privacy, sia un regolamento sull’uso della posta elettronica aziendale, che indichi i limiti dell’utilizzo di tale strumento ed i potenziali controlli che potranno essere effettuati dal datore e le relative e graduali modalità con cui tali controlli verranno posti in essere.

Le sentenze della Cassazione

In materia di controlli, sul piano giuslavoristico, **la Cassazione civile, Sez. lavoro, Sent. n. 25732 del 22.09.2021, ha posto la distinzione tra i controlli difensivi in senso lato e in senso stretto**: “occorre perciò distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell’art. 4 novellato in tutti i suoi aspetti e **“controlli difensivi” in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili** – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro. 32. Si può ritenere che **questi ultimi controlli**, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, **si situino, anche oggi, all’esterno del perimetro applicativo dell’art. 4.** […] 40. Inoltre, e il punto è particolarmente rilevante nel caso in esame, per essere in ipotesi

legittimo, il controllo "difensivo in senso stretto" dovrebbe quindi essere mirato, **nonché attuato ex post**, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto, sicché non avrebbe ad oggetto l'attività" – in senso tecnico – del lavoratore medesimo. Il che è sostanzialmente in linea con gli ultimi approdi della giurisprudenza di questa Corte, più sopra richiamati, in materia di "controlli difensivi" nella vigenza della superata disciplina."

In particolare, in materia di controlli difensivi in senso stretto, la Cassazione, Sez. Lavoro, n. 18168 del 26.6.2023 ha confermato come "il controllo "difensivo in senso stretto" deve essere "mirato" ed "attuato ex post", ossia "a seguito del comportamento illecito di uno o più lavoratori **del cui avvenuto compimento il datore abbia avuto il fondato sospetto**", perché solo a partire "da quel momento" il datore può provvedere alla raccolta di informazioni utilizzabili (Cass. n. 25732/2021 cit., punti 40 e 44)."

Sostanzialmente, se ne desume che, affinché il datore di lavoro possa accedere alla e-mail del dipendente, e quindi nella sua sfera coperta dalle garanzie costituzionali, occorre che il controllo sia mirato e avvenga ex post, ossia a seguito del fondato sospetto che il lavoratore abbia posto in essere un comportamento illecito. Oltre a ciò, occorrerà verificare contestualmente che siano stati ottemperati gli adempimenti in ambito privacy di informazione e trasparenza nei confronti del personale aziendale.

La sentenza n. 1870/2024 del Tribunale di Roma: un passo in più

Nonostante l'orientamento giurisprudenziale e l'interpretazione del Garante siano posti su piani diversi (sebbene intrecciati), una recente pronuncia dell'Autorità giudiziaria ne impone quantomeno una interpretazione più "rigorosa", orientata ad obbligare il datore di lavoro a seguire i capisaldi normativi e giurisprudenziali sinora citati.

Il Tribunale di Roma, in una recentissima sentenza n. 1870 del 14 febbraio 2024, ha dichiarato la nullità del licenziamento intimato dalla società, a seguito di un accesso illecito alle e-mail di un suo dipendente.

Nell'accogliere tale ricorso, il Tribunale ha precisato le modalità nonché i limiti entro cui possono essere effettuati i controlli, confermando altresì come l'accesso illecito alla corrispondenza sia avvenuto in contrasto con la normativa applicabile.

In tale pronuncia, il giudice di merito ha confermato quanto pronunciato dalla Cassazione, affermando come i controlli debbano avvenire non solo ex post, ossia successivamente all'insorgere di un fondato sospetto che giustifichi tale accesso, ma anche che solo le notizie successive al legittimo controllo possono essere utilizzate a fini disciplinari.

Come evitare i campi minati

In conclusione, per evitare i campi minati o quanto meno limitare danni e feriti occorre che l'azienda abbia posto in essere gli opportuni presidi organizzativi, in termini di procedure interne volte a regolamentare gli accessi alla casella di posta elettronica, definendone il perimetro e i limiti dell'accesso oltreché individuare i soggetti da coinvolgere, tra cui sarebbe buona prassi far rientrare l'ufficio privacy o il dpo o, in assenza, anche mediante l'ausilio di consulenti esperti qualificati. Inoltre, occorre verificare che siano rispettati, oltre alle menzionate norme dello Statuto dei lavoratori, anche i principi generali del trattamento, tra cui il principio di limitazione delle finalità e minimizzazione dei dati, oltre a verificare che sia stata rilasciata idonea informativa in merito al trattamento dei dati relativi alla posta elettronica.

Valuta la qualità di questo articolo

C

Marco Catalano

Avvocato, Consulente privacy

Seguimi su