TRIMESTRALE DI INFORMAZIONE E CULTURA DELL'ASSOCIAZIONE ITALIANA PER LA DIREZIONE DEL PERSONALE

dal 1980
NUMERO
marzo 2016 176

Dp Direzione del Personale

AIDP
ASSOCIAZIONE ITALIANA PER LA DIREZIONE DEL PERSONALE

HR AGILITY

Prospettive, competenze, opportunità di una funzione che, dopo il cambiamento, è pronta per cambiare ancora

IL CASO BARBULESCU

IL CONTROLLO DELLA POSTA ELETTRONICA E RECENTI MODIFICHE ALL'ART. 4 DELLO STATUTO DEI LAVORATORI

Luca Failla
Avvocato, Founding Partner, Lablaw Studio Legale.

di Luca Failla l.failla@lablaw.com

Il settore delle nuove tecnologie e della regolamentazione del lavoro è in continua evoluzione. Non passa giorno che non venga segnalato in Italia o all'estero un caso che evidenzia il (tutt'ora) difficile e non ancora definito rapporto fra *privacy* del dipendente e normativa regolatoria nel rapporto di lavoro. È solo di qualche giorno fa la recente sentenza della Corte europea dei diritti dell'uomo di Strasburgo sul caso Barbulescu, dove un lavoratore rumeno aveva lamentato la violazione del proprio diritto alla privacy nell'uso della posta elettronica da parte del proprio datore di lavoro che l'aveva poi licenziato.

Rigettato il ricorso avanti ai giudici nazionali, il lavoratore aveva poi citato in giudizio il proprio paese avanti alla Corte dei Diritti dell'Uomo di Strasburgo, richiedendo il risarcimento dei danni a suo dire derivatigli dalla mancata implementazione nel proprio paese di una adeguata protezione in tema di *privacy* in particolare sull'uso della posta elettronica aziendale.

Nella pronuncia ormai famosa la Corte ha però rigettato la pretesa del Barbulescu ritenendo nel caso specifico perfettamente osservata la normativa nazionale anche a protezione dei lavoratori e ciò poiché la posta elettronica era aziendale come definita dalle chiare norme "di ingaggio" aziendali (era stato proprio il datore di lavoro a chiedere al dipendente di aprire una casella di posta aziendale per poter rispondere meglio alle esigenze della clientela) e che il Barbulescu era stato licenziato per averla utilizzata in modo improprio (messaggi personali inviati e ricevuti alla/dalla fidanzata, amici e parenti) durante l'orario di lavoro ed in modo continuativo ed eccessivo.

La sentenza come spesso accade ha destato scalpore con commenti allarmati da parte di molti sulla *privacy* violata, ma tutto ciò non ha molto senso una volta calata nel contesto.

La Corte si è limitata ad affermare ciò che tutti sanno per buon senso prima ancora che per diritto: e cioè che gli strumenti aziendali (normalmente e salvo eccezioni che devono essere specificate) si utilizzano - e sono assegnate ai lavoratori - per motivi di lavoro e devono pertanto essere utilizzate a tali fini. ➤

"Nessun dipendente si permetterebbe di utilizzare la carta intestata dell'azienda per scrivere al proprio amministratore di condominio o per inoltrare un reclamo alla propria assicurazione o compagnia telefonica"

Eventuali eccezioni o tolleranze devono essere espressamente autorizzate dalle aziende.

Lo scrivo e lo ripeto da anni: nessun dipendente si permetterebbe mai di utilizzare la carta intestata dell'azienda in cui lavora per scrivere al proprio amministratore di condominio ovvero per inoltrare un reclamo alla propria assicurazione o compagnia telefonica, perché a tutti è nota la differenza fra scrivere a nome personale o a nome dell'azienda (ciò che avviene quando si utilizza la carta intestata dell'azienda).

Nessuna differenza vi è né vi deve essere con la posta elettronica che altro non è che la "carta intestata elettronica" dell'azienda per cui si lavora.

Del resto che così fosse in Italia è noto da tempo agli addetti ai lavori: nel lontano 2002 già il Tribunale di Milano aveva risolto un caso simile di una dipendente che, licenziata per giusta casa a seguito di messaggi (violazione della concorrenza) rinvenuti dal proprio datore di lavoro nella posta elettronica di questa mentre la stessa era assente dal lavoro, aveva pensato bene di denunciare il datore di lavoro lamentando il reato di "violazione della corrispondenza" di cui all'art. 616 del codice penale.

Ebbene in quella occasione il Gup di Milano aveva chiarito senza ombra di dubbio che nessun reato era possibile, trattandosi non di posta personale della dipendente ma di posta aziendale, come era chiarissimo dal nome associato alla casella di posta elettronica.

Il tutto – badate – in assenza pure di chiare regole di "ingaggio" da parte del datore di lavoro, e cioè pure in assenza di chiare policies aziendali come invece pretende il Garante della privacy (cfr *Linee guida per posta elettronica e internet* del 1° marzo 2007) e come è bene sempre introdurre in azienda sia per la posta elettronica sia per ogni altro strumento elettronico (o meno) in dotazione ai dipendenti per lo svolgimento dell'attività lavorativa.

Quindi almeno con riferimento alle email aziendali le cose sono più semplici di quel che appare, purchè siano chiare in azienda le *policies* di utilizzo della stessa ed i confini fra lecito e illecito.

Ma non sempre è tutto così scontato, soprattutto alla luce dei recenti cambiamenti legislativi che hanno interessato anche l'Italia con il recente Jobs Act.

Come tutti sanno il D.Lgs. n.151/2015 attuativo delle disposizioni della L.10 dicembre 2014, n. 183 (Jobs Act) in materia di controlli a distanza ha riscritto l'art. 4 St. Lav. con l'auspicabile scopo di renderlo più "vicino" alle realtà aziendali dopo oltre 40 anni dalla sua emanazione.

Al di là della struttura di fondo che non è cambiata, sono intervenute però importanti novità sia sul piano della flessibilità di utilizzo degli strumenti informatici per le aziende sia sul piano della effettività dei controlli e sanzioni nei confronti della produttività/performance dei propri dipendenti.

In generale, è ovviamente rimasto l'impianto di base già contenuto nell'art. 4 dello Statuto: necessario accordo con RSA/RSU a livello aziendale (ovvero dell'autorizzazione della Direzione territoriale del lavoro o Ministero del Lavoro, in assenza di accordo sindacale o in mancanza di organismi dei lavoratori in azienda) per l'instal-

lazione di apparecchiature che possano portare ad un controllo anche a distanza sull'attività dei lavoratori con l'eccezione tuttavia innovativa delle apparecchiature "utilizzate" dai lavoratori ed a loro affidate per l'esercizio dell'attività lavorativa, quali *tablets*, personal computer, *smartphone*.

In buona sostanza, e con una sana apertura al buon senso pratico, gli strumenti tecnologici c.d. "mobili" (pc, *tablet*, *smartphone*, cellulare) potranno essere utilizzati dai lavoratori (ed istallati dalle aziende) senza necessità di accordo con le RSA/RSU ovvero autorizzazione amministrativa; che peraltro è quello che è successo in questi anni, in cui nessuna azienda ha mai negoziato con le rappresentanze interne l'utilizzo di tali apparecchiature.

Analoga disposizione vale altresì per *"gli strumenti di registrazione degli accessi e delle presenze"* dei lavoratori sul lavoro, quali *badges* e tessere di accesso a locali delle aziende (quali aree parcheggio et *similia*), che anch'esse potranno essere installate in azienda in assenza di accordo sindacale o autorizzazione amministrativa.

Su tale nuovo e più preciso contesto normativo il Legislatore del Jobs Act ha introdotto una norma di chiusura particolarmente importante e significativa del nuovo corso nella regolamentazione del lavoro, precisando a chiare lettere che tutte le informazioni e i dati (purché correttamente raccolti sotto il profilo della *privacy*: informativa, raccolta del consenso, pertinenza) derivanti dall'applicazione dei nuovi strumenti informatici – sia che vengano raccolti con accordo sindacale/autorizzazione DTL, sia in assenza nei casi a ciò autorizzati – ben potranno essere utilizzati dal datore di lavoro *"a tutti i fini connessi al rapporto di lavoro"*, beninteso ivi incluso quello disciplinare e di controllo sull'esatto adempimento della prestazione lavorativa e ciò *"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"*.

Appare chiaro però che, così formulata, la norma apre nuovi scenari sia sul piano delle regole di condotta sia sul piano delle norme disciplinari.

Con la conseguenza che da qui in avanti nessun accordo sindacale potrà più prevedere come in passato (né autorizzazione amministrativa potrà essere rilasciata alla condizione) che i dati raccolti dalla installazione non vengano utilizzati a fini disciplinari, in quanto tale esclusione sarebbe in contrasto con quanto oggi prevede il novellato art. 4 dello Statuto.

Cade a questo punto un tabu che aveva resistito per quasi 50 anni, quello della impunità dei comportamenti illeciti dei lavoratori allorché provati con le apparecchiature informatiche.

Ed è questa una conseguenza dei tempi che stiamo vivendo: se pretendiamo dalla pubblica amministrazione di sanzionare i fannulloni ed i "furbetti" (filmati mentre timbrano il badge in mutande o in pigiama!) non possiamo che chiedere al sindacato comportamenti altrettanto coerenti con i dipendenti dell'industria privata sino ad oggi protetti dall'impunità disciplinare dei comportamenti illeciti comprovati mediante registrazioni o filmati.

È un cambio di mentalità importante a cui tutti saremo chiamati ad adeguarci per il futuro. Si apre poi uno scenario nuovo con riferimento a tutti gli accordi sino ad oggi siglati e che alla luce della nuova norma le aziende ben potrebbero rinegoziare con il sindacato aziendale, ovvero nazionale, previa disdetta dei vecchi accordi ove occorra.

È una strada certamente sfidante su cui molte aziende tuttavia si stanno muovendo. Viviamo tempi di grande cambiamento e le aziende devono essere in prima linea a guidarlo. ■