NUOVE TECNOLOGIE E CONTROLLI SUI LAVORATORI: QUID IURIS?

di Luca Giacopuzzi – Avvocato in Verona
www.lucagiacopuzzi.it

1) Premessa – 2) La tutela dell'email aziendale – 3) Non solo posta elettronica: controlli consentiti e controlli vietati

1) Premessa

E'indubbio che in un contesto aziendale un utilizzo dissennato degli strumenti informatici attribuirebbe al datore di lavoro un potere di controllo sui lavoratori talmente invasivo da compromettere la dignità e la riservatezza del dipendenti stessi.

Il tema, sebbene di stretta attualità, non è ancora stato oggetto di una regolamentazione che lo disciplini compiutamente.

In attesa, dunque, che si disegnino i confini normativi per un corretto rapporto tra tecnologia, impresa e lavoro, al momento tocca all'interprete individuare il punto di equilibrio tra il diritto del lavoratore al rispetto della propria sfera privata e quello, opposto, del datore di monitorare l'attività del dipendente, per evitare la commissione di illeciti. E lo sforzo interpretativo non è di poco conto.

Un aspetto molto dibattuto riguarda, ad esempio, la definizione dei limiti oltre i quali l'attività di controllo sarebbe illecita, perché attuata in spregio alle garanzie che il nostro ordinamento accorda al lavoratore (segnatamente a quelle tracciate dallo Statuto dei Lavoratori).

2) La tutela dell'email aziendale

E'ammissibile, per esempio, controllare la posta elettronica del dipendente, in sua assenza? Il quesito, sul quale gli imprenditori si interrogano con sempre maggior frequenza, impone un breve approfondimento.

La risposta non può che essere ricercata nelle norme di legge.

Partiamo, perciò, da un dato normativo: l'art. 5 L.547/93. Che recita testualmente: "Per corrispondenza si intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

La giurisprudenza amministrativa (cfr. T.A.R. Lazio, Sez. I, 15.11.01 n 9425), del resto, ribadisce che la posta elettronica deve essere tutelata alla stregua della corrispondenza epistolare ed è quindi caratterizzata dalla "segretezza". Sulla stessa lunghezza d'onda è il Garante per la privacy (si veda sul punto la Newsletter 12-18.07.99).

Ne consegue che è vietato leggere i messaggi se non si è i destinatari, pena l'applicazione dell'art.616 c.p., secondo il quale "chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta…è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno". Vi è di più. Si punisce anche chi, oltre che prendere cognizione, sottrae, distrae la corrispondenza, la sopprime o la distrugge.

Se quanto precede è un quadro – pur se sintetico – della tutela che il nostro ordinamento accorda alla corrispondenza (e dunque, come abbiamo visto, anche a quella inviata o ricevuta tramite posta elettronica), quando si parla di "e-mail aziendale" bisogna fare attenzione. E molta, perché in azienda lo scenario è parzialmente diverso.

Prendiamo le mosse da un caso concreto, un caso che potrebbe definirsi "ordinario". Questi, in estrema sintesi, i fatti.

Ad un'impiegata viene assegnata, come a tutti gli altri dipendenti, una casella di posta elettronica aziendale (nome.cognome@azienda.it). Durante l'assenza per ferie dell'impiegata, la sua responsabile ne controlla la posta e si imbatte in comunicazioni inerenti progetti di lavoro "personali", estranei cioè a quelli gestiti dalla dipendente per conto dell'azienda.

Ravvisando in tale condotta una violazione dei doveri relativi al rapporto di lavoro, il responsabile della società licenzia l'impiegata.

Quest'ultima, ritenuto violato il proprio diritto costituzionale alla segretezza della corrispondenza, impugna il licenziamento e sporge contestuale querela nei confronti della propria responsabile, per il reato di cui all'art. 616 c.p. (violazione di corrispondenza).

Il P.M. però avanza richiesta di archiviazione. La dipendente propone allora opposizione, che viene tuttavia respinta dal GIP, con un'ordinanza particolarmente significativa, divenuta presto "celebre".

Sostiene il GIP (cfr. ordinanza GIP Tribunale di Milano del 10 maggio 2002) che quanto affermato nell'art. 616 c.p. non può trovare applicazione con riferimento all'ipotesi di e-mail aziendale. La casella di posta elettronica, in altre parole, è sì tutelata, ma quando a metterla a disposizione è il datore di lavoro perde tutta la sua "riservatezza", in quanto strumento che l'azienda mette a disposizione del lavoratore al solo fine di consentirgli di svolgere la propria attività: come tale rimane nella completa e totale disponibilità del datore di lavoro, senza alcuna limitazione.

La mailbox aziendale - pur se "personale" (perché assegnata al singolo dipendente che ha un proprio "username" ed una propria "password" per accedervi) – deve quindi essere intesa come semplice "strumento di lavoro", e nulla più.

"Personalità" non significa necessariamente "privatezza", dal momento che l'e-mail aziendale, proprio perché tale, rimane bene aziendale, accessibile a tutti gli altri dipendenti autorizzati, ed al datore di lavoro in primis. La titolarità degli spazi di posta elettronica, pertanto, deve essere ricondotta esclusivamente all'azienda.

E'stato così precisato nella pronuncia che "il lavoratore che utilizza la casella di posta elettronica aziendale si espone al "rischio" che anche altri lavoratori della medesima azienda - che, unica, deve considerarsi titolare dell'indirizzo – possano lecitamente entrare nella sua casella e leggere i messaggi (in entrata e in uscita) ivi contenuti".

In conclusione, come è stato ben affermato (Aterno, in "No al controllo a distanza", Guida "La mia privacy", pag. 64 ss., Il Sole 24 Ore – 2004), il dipendente che utilizza l'indirizzo e-mail anche a fini privati ed extralavorativi non potrà invocare la segretezza della corrispondenza o impedire un controllo eccependo l'art. 4 dello Statuto dei Lavoratori, perché l'indirizzo non è privato, ma aziendale, e costituisce un semplice strumento messo a disposizione dell'utente-lavoratore dall'impresa per consentirgli di svolgere al meglio l'attività.

3) Non solo posta elettronica: controlli consentiti e controlli vietati

L'ordinanza del Tribunale di Milano prende posizione sui limiti di utilizzo "per scopi privati" degli strumenti aziendali (segnatamente, di quelli informatici) messi dal datore a disposizione del dipendente.

In uno scenario aziendale, però, la questione si allarga, per investire il più generale problema della determinazione dei limiti oltre i quali l'attività di controllo non è consentita.

In questa prospettiva assume particolare rilievo l'art. 4 L.300/70 (c.d. "Statuto dei Lavoratori"), che stabilisce in modo inequivoco il divieto di controllo a distanza (attuabile, ad esempio, tramite sistemi di videosorveglianza[1]).

La norma poc'anzi citata, al primo comma, così dispone: "E'vietato l'uso di apparecchi audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori".

La durezza del divieto è però mitigata al comma successivo, che – contemperando l'interesse del datore di lavoro alla produzione con quello del dipendente alla propria riservatezza – ammette la presenza in azienda di impianti e apparecchiature di controllo (ove – beninteso – l'installazione avvenga per esigenze produttive o di sicurezza del lavoro), dai quali derivi anche la possibilità di controllo a distanza dei lavoratori.

In tal caso, comunque, l'installazione di detti impianti è il momento conclusivo di un iter obbligato, che prevede l'accordo con le rappresentanze sindacali aziendali o, in mancanza, con la commissione interna.

A questo punto, giova dar conto di un'importante pronuncia giurisprudenziale che rileva ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza, tracciando una linea di demarcazione tra "controlli consentiti" e "controlli vietati".

Invertendo il precedente orientamento - il quale ricomprendeva all'interno del divieto ogni tipo di controllo sulle attività del lavoratore, comprensiva cioè della prestazione lavorativa e di tutti i comportamenti connessi (le c.d. "licenze comportamentali") - la pronuncia in precedenza citata (Cass., Sez. Lavoro, 3 aprile 2002 n. 4746) ha considerato leciti i c.d. "controlli difensivi", ossia quelli che non attengono all'attività lavorativa, ma che sono diretti ad accertare eventuali condotte illecite del lavoratore.

Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della L.300/70 – si afferma nella ricordata sentenza – è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi *certamente fuori dall'ambito di applicazione della norma* sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi, quali – ad esempio – gli apparecchi di rilevazione di telefonate ingiustificate).

Benchè, dunque, i controlli difensivi siano leciti, vi è da sottolineare la difficoltà operativa di predisporre un sistema di controllo che escluda in radice la possibilità di effettuare controlli diversi

[1] Non è questa la sede opportuna per una disamina dell'argomento. Sul tema della videosorveglianza si consultino, in particolare, due significativi provvedimenti del Garante Privacy: quello del 29.11.00 (c.d. "decalogo") e quello, più recente, del 29.04.04.

da quelli difensivi (il problema, all'evidenza, si pone in relazione agli impianti di videosorveglianza; è invece, ad esempio, agevolmente superabile laddove si faccia uso di tecnologie RFID per rilevare l'accesso ad aree riservate).

La disamina deve essere condotta con attenzione, poiché ove il controllo potesse aver ad oggetto la prestazione lavorativa, bisognerebbe necessariamente percorrere la strada indicata dal 2 comma dell'art.4 St.Lav.

Sebbene a parere di chi scrive – che , sul punto, trova conforto anche nella pronuncia della Suprema Corte poc'anzi esaminata - i controlli difensivi siano consentiti al datore di lavoro a prescindere da ogni trattativa a monte con le RSU, per completezza va ricordata la diversa opinione di chi (Aterno, Secco, tra gli altri) sostiene che anche detti controlli richiederebbero il vaglio della procedura contrattuale o autorizzativa prevista dall'art. 4, 2 co, St.Lav.

In ogni caso, appare evidente che – specie nell'attuale contesto storico-normativo, caratterizzato da una legislazione che non riesce a mettersi al passo con il progresso tecnologico - l'azienda dovrà adottare una politica aziendale trasparente, che espliciti con chiarezza al dipendente i limiti di utilizzo delle risorse informatiche assegnategli per lo svolgimento delle mansioni lavorative.

In attesa di un intervento chiarificatore a livello legislativo, questa sembra essere la via per contemperare equamente gli interessi in gioco: quello del dipendente a non subire arbitrarie intrusioni nella propria sfera privata e quello dell'imprenditore ad evitare la commissione di illeciti durante l'attività lavorativa.