

# Navigazione in Internet: no ai controlli difensivi senza accordo sindacale

Andrea Stanchi *Avvocato in Milano, Stanchi Studio Legale*



*La Cassazione scrive la parola fine (giudizialmente) su una vicenda che molto ha fatto discutere gli addetti ai lavori sul tema dei controlli a distanza inerenti l'utilizzo del Pc aziendale*

**Cass., sez. lav., 23 febbraio 2010, n. 4375**

Pres. Battimiello; Rel. Nobile; P.M. Matera; Ric. Re.; Res. La. Ca.

**Licenziamento - Navigazione in Internet - Controlli a distanza - Controlli difensivi - Limiti - Principi**

L'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, per cui tale esigenza non consente di espungere dalla fattispecie astratta dell'art. 4, c. 2, l. 300/1970 i casi dei cd. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso. In tale ipotesi si tratta, infatti, comunque di un controllo cd. preterintenzionale che rientra nella previsione del divieto flessibile di cui al c. 2 dell'art. 4 citato.

La sentenza da cui prende le mosse la vicenda è una acuta decisione del Tribunale di Milano (n. 1048/2004) poi confermata dalla Corte d'Appello (n. 668/2005) e infine dalla Cassazione. Sentenza nota perché iniziò un *revirement* sulla nozione di controlli difensivi elaborata da Cass. n. 4746/2002 secondo cui l'impiego di tecnologie di controllo per la tutela dei beni aziendali contro l'illecito non rientrava nelle previsioni dell'art. 4, l. 300/70. Si tratta di una delle prime affermazioni sui controlli delle navigazioni in Internet di una dipendente. Scoperti gli accessi con un applicativo software (Super Scout) la dipendente viene licenziata una prima volta, reintegrata e rlicenziata per navigazioni della medesima tipologia.

## La decisione della Cassazione

La Corte conferma la sentenza che ritiene inutilizzabili i dati relativi alle navigazioni perché ricavati da controlli in violazione del c. 2 dell'art. 4 Stat. Lav. che ammette i cd controlli a distanza preterintenzionali (cioè funzionali ad esigenze organizzative, produttive o di sicurezza) solo in presenza di accordo sindacale con la rappresentanza sindacale aziendale o di provvedimento del servizio ispettivo della Dpl. Del secondo dicono che è tardivo, assorbendo in ciò ogni questione. La Cassazione ritiene inammissibile la censura mossa per la qualificazione del fatto sotto il profilo dell'abuso del sistema informatico (art. 615-ter) perché non dedotta tra i motivi di appello, tra l'altro non essendo stato contestato l'accesso abusivo al sistema (la norma penale - si ricorda - copre sia l'accesso sia il trattenersi o l'uso *invito domino*), il quale presuppone regolamenti di disciplina analitici e non generici (sul che cfr. anche le *Linee Guida del Garante Privacy* del 2007). Giustamente la Corte invece glissa sulle affermazioni della Corte d'Appello sulla violazione dell'art. 8 S.L. (che infatti il primo giudice di merito aveva ritenuto - correttamente - non violato). Confermate anche le decisioni dei giudici del merito sul secondo recesso (basate sulla tardività). Sui controlli difensivi la Corte richiama il precedente della sentenza n. 15892/2007. In realtà poi ad andare a leggere bene la Corte si discosta dalle affermazioni di quella sentenza quando conferma le acute affermazioni della Corte milanese. Sul punto la decisione conferma la scelta dei giudici di merito che hanno ritenuto che «i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e **in via continuativa durante la prestazione** l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento». Cosa evidente laddove «nella lettera di licenziamento i fatti accertati mediante il programma Super Scout sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza sub specie di aver utilizzato tempo lavorativo per scopi personali (e non si motiva invece una particolare

*pericolosità dell'attività di collegamento in rete rispetto all'esigenza di protezione del patrimoni aziendali».* Per la S.C. sono poi fuori dalle contestazioni operate, cosiccome inconferenti, i richiami all'All. II, p. 3, della n. 626/1994 (ora All. XXXIV, p. 3, Tu 81/08), che non modifica la portata dell'art. 4 S.L. Non convincente e forse superficiale invece l'affermazione della Corte sull'irrilevanza concettuale dell'art. 615-ter sulla nozione dei controlli, come spieghiamo più avanti. Di routine poi le affermazioni su tardività, valutazione della prova riservata ai giudici di merito, novità di alcune censure, proporzionalità che richiedono spazi molto più ampi della presente notizia. La sentenza, che appare non particolarmente nuova sul tema o profondamente riflettuta, ha però dei certi profili di interesse laddove richiama la decisione dei giudici d'appello e fa propria la loro motivazione sopra riportata. Perché quelle affermazioni sottendono la necessità della distinzione tecnica di cosa sia una apparecchiatura di controllo nel mondo digitale (tema sul quale ho scritto ed a cui rinvio per la spiegazione estesa: «Apparecchiature di controllo, strumenti di comunicazione elettronica e controlli difensivi del datore di lavoro: diritti e doveri della digital citizenship nel digital workplace». <http://www.civile.it/news/visual.php?num=50961>).

### Gli strumenti di controllo nel mondo digitale

Occorre però intendersi sulla nozione di strumenti di controllo nel mondo digitale. La distinzione sta tra sistemi operativi (quelli che fanno funzionare il Pc) e sistemi applicativi (quelli che svolgono funzioni specifiche, come Super Scout). L'accertamento di condotte attraverso l'analisi dei dati dei sistemi operativi (log di sistema) da cui risulti il comportamento illecito del lavoratore è certamente estranea al sistema. Perché non si tratta di software applicativi che abbiano come propria funzione l'estrazione dell'aggregazione significativa di dati che trasformi l'elaboratore (strumento di lavoro) e lo concreti in una «*apparecchiatura di controllo*» nell'accezione considerata dalla legge ed intesa dai giudici milanesi. Diversamente ragionando, sarebbe come dire che non è possibile il controllo di conformità dell'esecuzione della prestazione, come risultato implicante anche il controllo sull'utilizzo proprio dello strumento di lavoro affidato. È un portato dell'era dell'informazione e della «cittadinanza digitale». E ciò vale per il prestatore di lavoro, ma anche per il datore di lavoro. Il quale, invece, si troverebbe privo di ogni strumento di verifica (più che lecita, non occulta, e non invasiva) dell'adempimento dell'obbligazione

### Stop al licenziamento

che il prestatore assume con il contratto. Si darebbe il caso che il solo mutamento dell'infrastruttura tecnologica determini l'illiceità del controllo (Giugni ricordava l'analogia con la verifica dell'operato delle segretaria a seguito dell'uso della dattilografia). Così non sono controlli ex art. 4 S.L. (e si può parlare di «controlli difensivi», ma sarebbe più coerente parlare di non controlli) quelli finalizzati alla tutela contro l'illecito penale ed alla ricostruzione della prova di esso. In modo particolare quando ciò riguardi la violazione dei sistemi informativi. Una simile conclusione è conforme a tutto il sistema (di ordine pubblico internazionale, specie dopo le affermazioni del Trattato di Lisbona, nuova norma fondamentale, sulla proprietà come diritto di libertà) degli ordinamenti a cui appartiene quello Italiano, ed è l'unica possibile secondo il principio (a cui costantemente si richiama la Corte Costituzionale, anche alla luce dell'art. 3) di **coerenza** dell'ordinamento giuridico, per cui non è possibile che ciò che è illecito per una parte di esso riceva protezione giuridica da altra parte, né è possibile ipotizzare che chi commetta un utilizzo illecito di uno strumento aziendale, punito penalmente dall'ordinamento, poi riceva da altra parte del-

l'ordinamento stesso una tutela soggettiva della sua posizione dolosamente illecita, come ritenuto anche dalla Corte Europea dei Diritti dell'Uomo (Caso KU c. Finlandia). Diverso è però se (come nel caso in commento) ciò che si utilizza per il controllo è un applicativo che ha come funzione l'estrazione dei dati in funzione di sorveglianza e monitoraggio della prestazione. Perché qui non si ha alcuna verifica di conformità a posteriori, ma un costante strumento di estrazione di dati che è funzionalmente destinato a produrre una «immagine» virtuale della prestazione, e per questa via, la violazione delle regole di cui alla norma. Insomma, il tema è delicato e complicato e richiede una meditazione adeguata alla evoluzione del sistema, specie laddove il contenuto di una norma incriminante deriva dal riferimento ad una nozione che muta al mutare della tecnologia di riferimento: la telecamera analogica del 1970 era molto diversa (ed unifunzionale) rispetto al Pc del 2010 (e qui soccorre il riferimento a Wittgstein ed al mutare del significato al mutare della tecnologia a cui è correlato). Non sono possibili scelte luddiste e non è possibile che il datore debba contrattare con terzi controinteressati il proprio diritto alla tutela dei beni (cioè il proprio diritto all'autodifesa, base di ogni sistema giuridico). Di un sistema che si evolve in senso di commettere all'impresa la tutela (penale) di svariate categorie di beni (leggi Dlgs n. 231/01) onerandola di strumenti adeguati di prevenzione e controllo sulla legalità dell'azione.