Lavoratori, controlli liberi

Il Jobs act liberalizza le verifiche su telefonini e pc dei dipendenti. Non servono più autorizzazioni o accordi. Ma occorre un regolamento aziendale per evitare abusi

DI MARINO LONGONI *mlongoni@class.it*

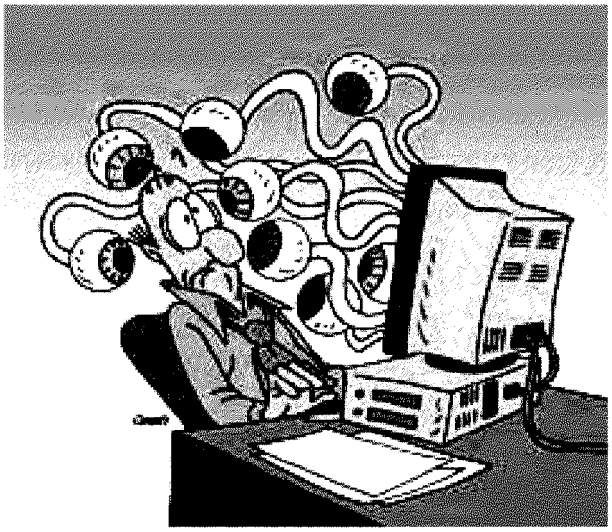
I lavoratori sono controllabili a distanza dal datore di lavoro senza necessità di alcuna autorizzazione né sindacale né amministrativa. D'altra parte i lavoratori sono comunque garantiti dalle regole poste a tutela della loro privacy. È questa la sintesi estrema di un dibattito estivo che si è infuocato dopo l'approvazione degli ultimi decreti legislativi sul Jobs act. Procediamo con ordine e cerchiamo di capire, concretamente, cosa cambia e quali sono i rischi che corrono i dipendenti nell'utilizzo dei più comuni strumenti aziendali: computer, telefonino ecc.

Si possono distinguere i controlli a distanza in due categorie. Da una parte, quelli effettuati con strumenti finalizzati esclusivamente al controllo del lavoratore. In questo caso non cambia nulla, questi controlli sono in linea di massima vietati.

Le novità introdotte con il Jobs act riguardano invece i controlli indiretti. Pensiamo all'utilizzo di strumenti sempre più comuni come le telecamere agli ingressi, i computer, i cellulari. Sono strumenti che hanno finalità produttive evidenti ma che, indirettamente, possono essere utilizzati anche per il controllo dei lavoratori.

Prima erano consentiti solo a certe condizioni (esigenze organizzative, sicurezza del lavoratore, tutela del patrimonio aziendale) e sulla base di un accordo collettivo o specifica autorizzazione della direzione territoriale del lavoro. Ora è intervenuta la liberalizzazione, nel senso che il datore di lavoro può fornire gli strumenti senza alcun problema. Non si tratta però di una liberalizzazione assoluta. Perché se il nuovo articolo 4 dello Statuto dei lavoratori non richiede più un preventivo controllo sindacale o amministrativo, restano pur sempre valide le norme previste dal codice della privacy e in particolare il provvedimento del Garante del n. 13 del 1° marzo 2007. La conseguenza è che, se il datore di lavoro vuole utilizzare questi strumenti anche per controllare la prestazione lavorativa, dovrà rispettare una serie di condizioni. Intanto deve predisporre e rendere noto ai dipendenti un regolamento aziendale che spieghi cosa si può e cosa non si può fare con questi strumenti. Poi dovrà effettuare i controlli nel modo meno invasivo possibile, e preceduti da un'informativa, oltre che proporzionati alla gravità della violazione che si intende verificare. Per esempio, il datore di lavoro dovrà preventivamente informare su come e quando saranno effettuati i controlli: indicando in ipotesi che una volta al mese saranno controllati, anche da remoto, tutti i computer aziendali e verranno eliminati tutti i file .exe. Anche i controlli sulla singola postazione devono rispettare il principio di gradualità, per cui prima si dovrà verificare per esempio quante ore si perdono su internet in un certo reparto, poi quanti siti si visitano, poi magari anche quali siti vengono visti da ogni singolo computer. Idem per la posta elettronica: vanno indicate le modalità d'uso e pure le modalità di controllo. Se ci fosse bisogno di aprire le caselle di posta elettronica del lavoratore, questo dovrà essere fatto in contraddittorio, alla presenza di un fiduciario del dipendente.

Sono ammessi i controlli difensivi, quelli cioè nei quali l'azienda cerca di determinare se un comportamento illecito è stato compiuto dal dipendente: in questo caso l'apertura della casella di posta elettronica del lavoratore è giustificata dalla giurisprudenza come esercizio di un diritto aziendale. Ma si tratta di una categoria diversa rispetto all'esercizio del controllo sulla produttività del dipendente.



In fin dei conti la riforma non fa altro che adeguare la disciplina normativa all'evoluzione della tecnologia utilizzata in azienda, ben diversa da quella degli anni 70. E pazienza se questo ha comportato anche il venir meno di qualche prerogativa alla quale i sindacati si erano affezionati.


ItaliaOggi
Lavoratori, controlli liberi
Sanzioni tributarie alleggerite

Norme sulla privacy come freno ai controlli abusivi su telefonini e tablet del dipendente

Resta solo lo scudo individuale

Pagina a cura
DI ANTONIO CICCIA MESSINA

Solo la privacy stoppa i controlli abusivi sui telefonini, tablet e cellulari e tutti gli altri strumenti di lavoro dati in uso al dipendente. Ma, in caso di uso indebito delle informazioni sul lavoratore fornite dai dispositivi, le tutele sono a posteriori e affidate al singolo lavoratore. È questa la conseguenza della modifica dell'articolo 4 dello Statuto dei Lavoratori attuata dal decreto cosiddetto Jobs Act sulla semplificazione del rapporto di lavoro.

La norma, infatti, elimina il filtro del controllo sindacale o dell'autorizzazione ministeriale sugli strumenti di lavoro e sui lettori di badge e bollatrici.

Certo viene mantenuto l'impianto delle tutele del Codice della privacy (dlgs 196/2003). Ma l'impostazione del nuovo articolo 4 dello Statuto dei lavoratori manda in soffitta una tutela preventiva collettiva (controllo sindacale) o amministrativa (autorizzazione ministeriale).

Quindi mentre prima del Jobs Act il lavoratore godeva di un doppio regime di tutela: quello collettivo/amministrativo (vecchio articolo 4 dello Statuto dei lavoratori) e quello individuale (codice privacy), ora c'è un solo livello di tutela.

E sul terreno del possibile conflitto abbiamo da una parte il datore di lavoro, che non ha più procedure (sindacali o ministeriali) da osservare per usare e far usare strumenti di lavoro, da cui derivi la possibilità di controllo a distanza; dall'altra parte c'è il singolo lavoratore, che dovrà agire come singolo per opporsi a condotte invasive del datore di lavoro. Certo il singolo dipendente potrà rivolgersi alla propria associazione sindacale per farsi assistere, ma solo dopo avere subito una violazione della sua privacy.

La regola è che il datore di lavoro lo può fare (usare e far usare strumenti di lavoro che sono anche strumenti di controllo indiretto), senza burocrazia sindacale o ministeriale (questa è la semplificazione), ma incorre in responsabilità se attenta alla riservatezza del dipendente.

La semplificazione sta anche nel fatto che è amplissima la possibilità di intendere un certo strumento come strumento di lavoro. Si noti che il nuovo articolo 4 non parla di strumenti «necessari» o «indispensabili» per la mansione: qualunque strumento di fatto utilizzabile per la prestazione lavorativa, può essere usato senza controllo preventivo.

Su questo, dunque, il potere organizzativo da parte del datore di lavoro avrà una priorità: è il datore di lavoro che, in relazione a standard produttivi individua gli strumenti utili per la mansione. Una stessa mansione potrà essere svolta con dispositivi di diverso contenuto tecnologico e appartiene alla discrezionalità del datore di lavoro scegliere lo strumento.

Una volta scelto dal datore di lavoro, quello strumento diventa utile. Certo uno strumento non può diventare utile, solo perché con esso si può realizzare un controllo indiretto, ma la tecnologia delle informazioni è tale da consentire la raccolta di informazione attraverso potenzialmente tutti i dispositivi di lavoro e, quindi, è facile prevedere un progressivo allargamento della categoria degli strumenti utili per la mansione nel contempo raccoglitori di dati.

Sburocratizzazione a parte, rimane lo sbarramento privacy. Da questo punto di vista va notato che la versione ultima si differenzia molto da una versione iniziale in cui l'allora bozza di decreto legislativo prevedeva la possibilità di libero utilizzo delle informazioni raccolte «a tutti i fini connessi al rapporto di lavoro»: un inciso che, di per sé, avrebbe autorizzato il datore di lavoro ad usare le informazioni raccolte con gli strumenti di lavoro per sanzioni disciplinari, licenziamenti trasferimenti, o anche in positivo per promozioni, insomma per tutto quanto previsto dal rapporto di lavoro.

Si noti che l'autorizzazione all'uso «per ogni finalità» era nella norma e questo avrebbe aperto la strada alla discussione della sopravvivenza delle disposizioni sulla privacy o di una loro abrogazione per effetto della norma che facoltizzava qualsiasi uso da parte del datore di lavoro.

I chiarimenti del ministero del lavoro e la riformulazione del testo consentono, tuttavia, una lettura più garantista.

Per esempio, invocando, come ha fatto il ministero del lavoro (si veda *ItaliaOggi* del 19 giugno 2015), la distinzione tra dispositivi e applicativi.

Secondo il ministero, l'accordo sindacale o l'autorizzazione ministeriale non ci vuole se, e nella misura in cui, lo strumento viene considerato quale mezzo che «serve» al lavoratore per adempiere la prestazione.

Da ciò deriva che, nel momento in cui lo strumento di lavoro viene modificato (per esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione.

Allora da strumento che «serve» al lavoratore per rendere la prestazione il pc, il tablet o il cellulare diventano strumenti che servono al datore per controllarne la prestazione.

Quindi, se il datore di lavoro modifica lo strumento di lavoro con applicativi da cui possa derivare un controllo indiretto, lo potrà fare, ma solo alle condizioni generali: sussistenza di esigenze organizzative e produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale; accordo sindacale o autorizzazione.

Seppure non esplicitata dal testo della norma, la precauzione suggerita dal ministero del lavoro trova riscontro nel provvedimento del garante della privacy dedicato all'uso di internet e posta elettronica sui luoghi


LA RIFORMA DEL LAVORO
Resta solo lo scudo individuale

di lavoro (Deliberazione n. 13 del 1° marzo 2007), nella parte in cui prescrive che resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati «in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori».

Sarebbe bastato riprendere quella formulazione per fugare ogni dubbio, mentre, con il testo licenziato, si dovrà aspettare che le sentenze si orientino in un senso o nell'altro.

Anche qui la norma di tutela deriva da una fonte che si occupa di privacy e si tratterebbe di contenziosi a posteriori (e cioè dopo che il datore di lavoro ha disposto l'uso di un certo dispositivo).

L'assenza di informativa rende i dati inutilizzabili

Il nuovo art. 4 dello Statuto dei lavoratori estrapola dal Codice della privacy una tutela specifica per il lavoratore e formula, poi, un richiamo generalizzato alle disposizioni del medesimo codice. L'articolato del Jobs Act afferma che le informazioni raccolte dagli strumenti di lavoro sono utilizzabili a condizione che sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto del codice della privacy. Seppure la disposizione faccia riferimento ai dati personali raccolti con gli strumenti di lavoro, è ovvio che la privacy va rispettata dal datore di lavoro a prescindere dal mezzo utilizzato per la raccolta dati.

In ogni caso, la prima conclusione è che qualora il lavoratore non sia stato adeguatamente informato dell'esistenza e delle modalità d'uso delle apparecchiature di controllo e delle modalità di effettuazione dei controlli, allora, i dati raccolti non sono utilizzabili a nessun fine, nemmeno a fini disciplinari.

In sostanza l'uso da parte del datore di lavoro delle informazioni raccolte mediante gli strumenti di lavoro (per fini connessi al rapporto di lavoro) è, comunque, subordinato alle regole del codice della privacy (che riguardano anche l'informativa, cautela, questa, duplicata nel Jobs Act). Vediamo, dunque, il panorama delle garanzie scritte nel provvedimento del garante n. 13 del 1° marzo 2007, pubblicato sulla *G.U.* n. 58 del 10 marzo 2007, che rimangono tutte valide, e che servono da principi generali, sebbene il provvedimento sia limitato ad alcuni dispositivi (riguarda infatti l'uso di internet e della posta elettronica).

Il Garante prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta, poi, la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori.

Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda. Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è, inoltre, chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori. Per quanto riguarda internet è opportuno ad esempio: • individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa; • utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.

Per quanto riguarda la posta elettronica, è opportuno che l'azienda: • renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza; • valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato a un uso personale; • preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi; • metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate

all'attività lavorativa. Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.