I pc dei dipendenti sono controllabili?

Autore : Valentina Azzini

Data: 13/03/2019

> ***Via libera al controllo del pc assegnato al dipendente quando è finalizzato a tutelare l'azienda. Rimane illegittimo, invece, il controllo a distanza del lavoratore e del suo operato, della posta elettronica che invia e riceve, se questo non è giustificato dalla repressione di condotte illecite***

L'azienda per cui lavori ti ha assegnato un pc per consentirti di svolgere le tue

mansioni in ufficio, oppure fuori sede. Con quel computer hai sì lavorato, ma nei momenti di pausa o scarso lavoro hai scaricato il referto delle tue ultime analisi cliniche, hai letto alcune mail personali, hai navigato in internet per motivi personali; hai quindi ricevuto una contestazione disciplinare dal tuo datore perché, controllando la cronologia della navigazione in internet e i documenti scaricati, ha visto che hai visitato siti non pertinenti al tuo lavoro e ti domandi se questo controllo aziendale fosse lecito. Il **potere di controllo del datore sul pc del dipendente** è possibile, ma solo in casi particolari, quando questo sia necessario a tutelare l'azienda e la sua immagine, oppure quando sia indispensabile per difendersi in giudizio. Il **controllo datoriale**, invece, non può avvenire senza motivo e nemmeno per controllare la qualità del lavoro svolto dal dipendente. A maggior ragione, il controllo aziendale non deve violare la **privacy del lavoratore**. Vediamo allora quando e fino a che punto **i pc dei dipendenti sono controllabili**.

Il Jobs Act e il potere di controllo aziendale

Il Jobs Act ha rimodulato la disciplina in materia di **divieto di controlli aziendali** a distanza, essendo necessario, al giorno d'oggi, conciliare la tutela delle aziende, il lavoro dei dipendenti, la privacy e l'utilizzo degli strumenti tecnologici messi a disposizione dei lavoratori.

Si pensi al telefono cellulare aziendale assegnato al lavoratore che, avendo il gps integrato, potrebbe consentire all'azienda di controllarne gli spostamenti, oppure l'attribuzione di una casella di posta elettronica aziendale sulla quale in lavoratore, sprovvisto in indirizzo email proprio, riceva anche comunicazioni personali, quali referti medici, o bollette delle utenze di casa.

Tra i dispositivi utilizzati dal lavoratore per svolgere la prestazione lavorativa abbiamo infatti non solo pc, smartphone e tablet, ma anche la rete internet aziendale.
Mentre per tutti i dispositivi che consentono potenzialmente un controllo indiretto a distanza del lavoratore è necessario che l'azienda, per utilizzarli legittimamente, sottoscriva un accordo sindacale o riceva l'autorizzazione del garante della privacy, per gli strumenti di lavoro quali pc, smartphone, tablet, nonché per la rete aziendale, le imprese sono oggi obbligate ad effettuare un inventario degli strumenti di lavoro affidati ai dipendenti ed informare specificamente i lavoratori su come si usano e sui tipi di controlli che potrebbero essere effettuati.

Questo può avvenire o mediante l'organizzazione di **riunioni mirate**, oppure – meglio ancora – scrivendo un **regolamento aziendale, o policy aziendale**, che ben disciplini l'utilizzo dei beni aziendali e precisi quali controlli potranno essere effettuati

dal datore.

Tale policy dovrà quindi essere portata a conoscenza dei dipendenti e possibilmente da questi **sottoscritta per accettazione**.

I controlli ammessi

Vi sono alcune ipotesi in cui il **controllo aziendale** sui dispositivi affidati ai dipendenti si considera **lecito**, in quanto finalizzata alla tutela del patrimonio aziendale e alla difesa degli interessi del datore.

Si tratta, ad esempio, dei **controlli difensivi**, che di per sé, non sono finalizzati a vendere come il dipendente lavora, ma se lavorando sta creando un danno all'azienda, del quale questa intende chiedere il risarcimento: si pensi al lavoratore che crea un falso profilo facebook per ledere l'immagine aziendale; oppure il controllo circa gli spostamenti del lavoratore, a seguito di ripetute segnalazioni ricevute da clienti che lamentano di non vedere l'agente che dovrebbe recarsi da loro settimanalmente, da diverso tempo.

Sono ammessi altresì controlli mediante **servizi di investigazione** volti a verificare, ad esempio, se un dipendente passa la maggioranza delle sue ore lavorative su internet per scopi personali, arrecando così un danno economico all'azienda che lo sta pagando senza che questi lavori.

I risultati dei controlli svolti dall'azienda, potranno però essere utilizzati per sanzionare il dipendente, oppure per agire giudizialmente nei suoi confronti solo a **due condizioni**:

- che sia stata fatta informazione al lavoratore su come si usano i dispositivi forniti e sui tipi di controlli effettuati;
- che sia rispettato il codice della privacy

I controlli vietati

Sono invece sempre **vietati i controlli a distanza** e cioè i controlli svolti all'insaputa del lavoratore, con strumenti invasivi: ad esempio è vietato installare una telecamera sull'auto o nell'ufficio del lavoratore per controllare se effettivamente lavora.

Sono altresì **vietati i controlli indiscriminati** sulle email aziendali e sull'uso di internet: i controlli, come detto, possono essere svolti solo se sono giustificati da una

finalità lecita, come ad esempio la tutela di un diritto che si intende azionare davanti al giudice (ad esempio per dimostrare che il lavoratore ha rubato in azienda, oppure ha svolto attività in concorrenza con l'azienda).

Se il datore vuole valutare la **qualità dei servizi offerti** dai propri dipendenti (si pensi ad esempio al controllo circa la preparazione e la cortesia degli operatori di call center quando ricevono chiamate dagli utenti/clienti), può farlo purchè però i **controlli** siano **anonimi**.

Il **Garante della privacy** ha inoltre vietato la registrazione di tutte le email in uscita, il monitoraggio costante dei siti internet visitati dal lavoratore, la copia di tutti i file salvati dal dipendente tramite propria chiavetta Usb: questi controlli possono essere svolti **solo in presenza di motivi specifici** e gli accertamenti **non devono essere sistematici, indiscriminati e preventivi**.

Infine, controlli fatti sulla posta elettronica e sull'uso di internet dei dipendenti sono leciti solo se è stato adottato e diffuso in azienda un apposito **regolamento o policy in materia di sicurezza informatica**, che consenta ai lavoratori di sapere cosa possono fare e cosa non possono fare con il pc che gli viene assegnato e le conseguenze disciplinari che un uso no0n consentito possa comportare.