Controllo sui lavoratori : strumenti di lavoro e strumenti di rilevazione accessi e presenze

Le disposizioni del decreto legislativo 151/2015 conosciuto anche come Jobs Act, hanno modificato l'articolo 4 del vecchio Statuto dei lavoratori, costringono le imprese a riscrivere le Policy Aziendali, compresa quella sulla sicurezza informatica, in osservanza alle nuove procedure previste per il controllo dei lavoratori. La Job Act ha inserito una disciplina speciale per gli strumenti di lavoro e per gli strumenti di rilevazione accessi e presenze. Nello specifico l'articolo 23 del D.Lgs. n. 151/2015 si incarica di modificare l'articolo 4 della Legge n. 300 del 1970 – anche nota come Statuto dei Lavoratori – per rimodulare la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

Tra i dispositivi «utilizzati dal lavoratore per rendere la prestazione lavorativa» si trovano :

- Pc,
- smartphone,
- tablet
- ma anche la rete aziendale.

Mentre per tutti i dispositivi di controllo indiretto è necessario l'accordo sindacale o l'autorizzazione amministrativa.

- Per strumenti di lavoro (Pc, smartphone, tablet ... ma anche la rete aziendale) o di rilevazione accessi e presenze, la legge stabilisce una deroga espressa per il loro utilizzo, secondo la quale, le aziende sono obbligate ad effettuare un censimento degli strumenti di lavoro e fare informazione ai lavoratori su come si usano i dispositivi forniti e sui tipi di controlli effettuati, il tutto nel rispetto della codice della Privacy. Tutte indicazioni che devono essere presenti nella Policy sulla Sicurezza informatica di un'azienda.

Controlli Ammessi

- **sono ammessi i controlli difensivi**, che di per sé, non hanno come oggetto la prestazione lavorativa.

- **sono ammessi i controlli sui dispositivi** che possono essere utilizzati per scopi organizzativi/produttivi, sicurezza del lavoro o tutela del patrimonio aziendale e che possono fornire anche informazioni sulla prestazione o sulla condotta del lavoratore (ma non devono essere utilizzati a tale fine come scopo primario).

- **sono ammesse richieste di consulenza per servizi di investigazione atti a verificare, ad esempio, un eventuale falso profilo sui social network** che abbia danneggiato l'immagine aziendale o sistemi di controllo del traffico di rete finalizzati ad accertare condotte illecite dei lavoratori per determinare se un lavoratore passa la maggioranza delle sue ore lavorative su internet per scopi personali.

Con l'introduzione della Job Act è stato consentito al datore di lavoro di verificare le modalità di utilizzo degli strumenti ricevuti dal lavoratore, senza essere vincolato all'accordo sindacale preventivo, anche se le prove raccolte non sempre potranno essere utilizzate se l'azienda non ha redatto una Policy sulla Sicurezza informatica interna, poichè questa nuova facoltà del datore di lavoro risulta essere subordinata all'obbligo in capo al datore di lavoro di fornire un'adeguata informazione – ai lavoratori – delle modalità d'uso degli strumenti e dell'effettuazione dei controlli.
sono ammessi gli strumenti di rilevazione accessi e presenze senza la trattativa sindacale/procedura amministrativa.

Per quanto riguarda le informazioni raccolte a tale scopo, esse possono essere utilizzate per tutte le finalità connesse al rapporto di lavoro, anche per procedimenti disciplinari, ma solo a due condizioni:
1) che sia stata fatta informazione al lavoratore su come si usano i dispositivi forniti e sui tipi di controlli effettuati;
2) che sia rispettato il codice della privacy

Controlli Vietati

- **vietato il controllo a distanza, e cioè il controllo subdolo,** all'insaputa del lavoratore, con strumenti invasivi, che condizionano la libertà individuale

- **vietati i controlli preterintenzionali senza la trattativa sindacale/procedura amministrativa**.

- **Per i controlli preterintenzionali con strumenti a distanza è prevista una trafila sindacale e, in mancanza di accordo, una trafila burocratica** (autorizzazione della direzione territoriale del lavoro). Quindi prima di installare un sistema di telecamere, per esempio, si deve ricorrere all'accordo sindacale o all'autorizzazione amministrativa.

- **Il datore di lavoro non può effettuare controlli indiscriminati sulle email aziendali e sull'uso di internet:** i controlli possono essere svolti solo se sono giustificati da una finalità lecita, come la tutela di un diritto esercitabile in via giudiziaria (ad esempio la repressione di una condotta illecita del dipendente).

- **Non possono essere effettuati controlli prolungati, costanti o indiscriminati; devono essere preferiti, quando possibile, controlli anonimi e su dati aggregati, e le indagini devono essere circoscritte a specifiche aree di lavoro.**
- **Infine, devono essere cancellati periodicamente i dati relativi agli accessi a Internet e al traffico telematico.**
- **In base alle prescrizioni del Garante della privacy, non sono leciti la registrazione massiva di tutte le email in uscita, il monitoraggio costante dei siti internet visitati o la copia di tutti i file salvati dal dipendente tramite la porta Usb:** queste attività possono essere svolte solo in presenza di motivi specifici e gli accertamenti non devono essere sistematici, indiscriminati e preventivi.

- **Le indagini fatte sulla posta elettronica e sull'uso di internet dei lavoratori sono lecite solo se è stato adottato e diffuso in azienda la Policy sulla Sicurezza informatica**, tramite la quale i lavoratori possono informarsi nel dettaglio sulle regole da seguire. Il codice di condotta deve essere reso ufficiale e deve specificare in sintesi: l'uso che i lavoratori possono fare del computer aziendale, i limiti entro i quali è consentito o tollerato un uso privato del computer o cellulare in dotazione; i limiti d'uso della posta aziendale, e in particolare la possibilità o meno di un suo utilizzo per scopi privati; i siti internet la cui consultazione è vietata, perché sono considerati non correlati con la prestazione lavorativa; le conseguenze disciplinari applicabili in caso di uso contrario alla policy e molto altro ancora ... rinvenibile qui per approfondimenti : Policy sulla Sicurezza informatica

Policy Sulla Sicurezza Informatica o Regolamento Informatico Aziendale

La Policy sulla Sicurezza Informatica è quel documento nel quale sono contenute tutte le disposizioni, comportamenti e misure organizzative richieste ai dipendenti e/o collaboratori aziendali per contrastare i rischi informatici.

Rispettare il codice della privacy

Rispettare il codice della privacy significa adottare le precauzioni prescritte dal codice della privacy e dal Garante nel provvedimento del 1° marzo 2007. In particolare l'azienda dovrà:

- a) dettare un disciplinare interno (il disciplinare interno deve indicare il censimento degli strumenti di lavoro in dotazione del personale, le modalità di utilizzo dei dispositivi e la graduazione dei controlli);
- b) individuare le misure organizzative;
- c) individuare le misure tecnologiche;
- d) osservare il divieto di controllo diretto.

L'individuazione dei dispositivi come strumenti di lavoro è presupposto imprescindibile dell'utilizzabilità delle informazioni acquisite per tutti i fini connessi con il rapporto di lavoro in essere tra l'azienda ed il dipendente. È necessario quindi avere una documentazione come la Policy sulla Sicurezza informatica dalla quale emerga la destinazione d'uso dei dispositivi aziendali, nonché l'avere fornito ai lavoratori tutte le necessarie informazioni sul loro scopo. L'inosservanza delle prescrizioni del Garante sull'adozione del disciplinare interno è punita con sanzione pecuniaria amministrativa da 30 mila fino a 180 mila euro (art. 162, comma 2-ter, codice della privacy). Se non si osserva la prescrizione sull'obbligo di trattativa sindacale/autorizzazione amministrativa (art. 4, commi 1 e 2 della legge 300/1970) si applica la sanzione penale con una ammenda fino a 1549,37 euro o con l'arresto da 15 giorni a un anno.