Il controllo a distanza delle attività dei lavoratori

ANALISI GIURIDICA DELL'ISTITUTO

Nel nostro ordinamento sono presenti alcuni limiti per il datore di lavoro relativamente all'attività di vigilanza e controllo che può esercitare sui propri dipendenti. Esistono, infatti, il diritto alla riservatezza, la dignità personale, la libertà di pensiero, di espressione e di comunicazione.
Sul luogo di lavoro tali diritti sono tutelati dal Legislatore con **la legge 20 maggio 1970, n. 300** (Statuto dei Lavoratori), in particolare con gli **articoli 4** (Impianti audiovisivi e altri strumenti di controllo), **8** (Divieto di indagini sulle opinioni) e **15** (Atti discriminatori).
Tale disciplina è stata **riformatadal c.d. "Jobs Act", che ha modificato l'art. 4 dello Statuto dei lavoratori**.

Prima della riforma (entrata in vigore il 24 settembre 2015), **vigeva un divieto assoluto** di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Tale divieto veniva meno solo nei casi in cui il datore di lavoro, per esigenze organizzative, produttive o di sicurezza del lavoro, intendesse installare nuove apparecchiature dalle quali potesse derivare un controllo a distanza dell'attività lavorativa dei dipendenti: in tal caso, era necessario il previo accordo con le organizzazioni sindacali o, in mancanza, l'autorizzazione delle articolazioni locali del Ministero del Lavoro territorialmente competenti.

Il nuovo testo della norma pone in evidenza due aspetti:
1) da un lato, l'impiego di impianti audiovisivi e di altri

strumenti che consentono un controllo a distanza dell'attività dei lavoratori (quali impianti di videosorveglianza);
2) dall'altro, l'utilizzo di altri strumenti che il datore di lavoro assegna ai propri dipendenti per lo svolgimento della prestazione lavorativa (ad esempio, pc, telefoni, tablet), nonché gli strumenti di rilevazione degli accessi e delle presenze.

1) I primi (impianti audiovisivi e strumenti di controllo a distanza) continuano, come in passato, a poter essere utilizzati dall'imprenditore **esclusivamente per esigenze di carattere organizzativo e produttivo, di sicurezza del lavoro e di tutela del patrimonio aziendale**. Affinché la loro installazione ed il loro utilizzo sia considerato legittimo, è necessario che vi sia un accordo sindacale sulle modalità di utilizzo di tali apparecchiature (accordo stipulato, a seconda delle dimensioni dell'impresa, con le RSA o le RSU o con i sindacati comparativamente più rappresentativi sul piano nazionale). Se tale accordo manca, il datore di lavoro deve ottenere la previa autorizzazione della Direzione Territoriale del Lavoro o del Ministero del Lavoro (si rivolgerà all'uno o all'altro a seconda delle dimensioni dell'azienda).

2) La seconda parte della norma, invece, legittima l'esercizio di un controllo a distanza (c.d. diretto) effettuato sugli strumenti utilizzati dal lavoratore per eseguire le proprie mansioni e sugli strumenti di rilevazione degli accessi e delle presenze (c.d. lettori badge). In questo caso, infatti, **non c'è l'obbligo per il datore di lavoro di raggiungere una intesa sindacale o di ottenere l'autorizzazione ministeriale**: il controllo è libero e può essere effettuato anche senza un'esigenza organizzativa o produttiva. In assenza di qualsiasi funzione di "filtro" attribuita alle organizzazioni sindacali o alla vigilanza del Ministero del Lavoro per mezzo della Direzione Territoriale del Lavoro, **è il singolo lavoratore che dovrà verificare se il controllo è esercitato dall'imprenditore in modo legittimo** ed eventualmente recarsi

presso un sindacato o un legale per tutelare i propri diritti.

Oltre alla normativa giuslavoristica, il Datore di lavoro dovrà rispettare anche tutto l'impianto normativo relativo alla protezione dei dati personali, costituito dal **Regolamento Europeo 2016/679, dal Codice Privacy** (D.lgs. 196/2003) e dai provvedimenti emessi nel corso degli anni **dall'Autorità Garante per la Protezione dei Dati Personali.**
Per non incorrere in sanzioni penali e civili il Datore di Lavoro dovrà mettere in atto delle corrette procedure interne per la gestione di tali dati, in primo luogo dovrà rispettare il dettato normativo dell'art. 4 dello Statuto dei lavoratori che prevede, al comma III, la possibilità di raccogliere le informazioni mediante gli strumenti utilizzati per rendere la prestazione di lavoro e di poterne disporre per tutti i fini connessi al relativo rapporto, purché sia stata fornita adeguata informazione al lavoratore sulle modalità d'uso dei dispositivi stessi e sui possibili controlli, il tutto nel rispetto dei principi sanciti dalla normativa vigente in tema di privacy.

Il datore di lavoro dovrà pertanto essere in grado di dimostrare come **l'utilizzo delle tecnologie informatiche non rientri in un programma volto esclusivamente al controllo dell'attività del lavoratore**. È bene ricordare che il controllo a distanza non sussiste solamente in presenza di impianti di videosorveglianza, ma anche in presenza di attività quali "la conservazione e la categorizzazione dei dati personali dei dipendenti relativi alla navigazione in internet, all'utilizzo della posta elettronica ed alle utenze telefoniche da essi chiamate", come ribadito anche da una recente sentenza della Corte di Cassazione (sentenza 28.05.2018 n.13266).
L'uso degli strumenti di controllo dev'essere sempre contenuto nella portata e proporzionato.

Affinché il controllo a distanza possa ritenersi legittimo e i dati così acquisiti siano utilizzabili, è fondamentale f**ornire**

ai dipendenti un'informativa esaustiva in ordine all'uso degli strumenti aziendali, ai dati trattati, al loro utilizzo e conservazione, nonché circa le modalità con cui vengono eseguiti i controlli, che i controlli non abbiano ad oggetto l'attività lavorativa del dipendente e che siano effettuati ex post, a seguito del verificarsi di un comportamento illecito del lavoratore o comunque per la verifica di un'anomalia del sistema informatico. Non è infatti consentito un accesso indiscriminato al datore di lavoro agli strumenti informatici in uso al lavoratore.

I lavoratori devono essere sempre **previamente informati del possibile controllo datoriale sulle loro comunicazioni anche via internet**; per questo motivo diventa fondamentale adottare una privacy policy adeguata e calata nello specifico contesto e sarà perciò compito del datore di lavoro fornire al lavoratore una adeguata informativa relativa il trattamento dei dati personale (ex art. 13 Regolamento Europeo 2016/679). Qualora il Datore di Lavoro contravvenga alle prescrizioni previste dal GDPR o dallo Statuto dei Lavoratori, potrà incorrere in sanzioni di carattere amministrativo e penale.

Trattamento dei dati biometrici: che cosa prevede il GDPR

A disciplinare il trattamento dei dati biometrici per applicazioni di controllo accessi e rilevazione presenze sono il GDPR – General Data Protection Regulation e il successivo **decreto italiano di adeguamento (D.lgs. 101/2018).**

L'art. 9, par. 1, del GDPR **vieta – in linea generale – il trattamento dei dati biometrici, fatte salve alcune eccezioni**. La prima eccezione prevede che l'interessato abbia autorizzato il trattamento.

Seguono, poi, **altre eccezioni**, che consentono l'utilizzo dei dati biometrici solo se necessario in ambito lavorativo o nell'ambito della sicurezza sociale e collettiva; se necessario per la protezione di un interesse vitale

dell’interessato o di altra persona; se necessario in un procedimento giudiziario; se vengono rilevati particolari motivi di interesse pubblico o per motivi di sicurezza sanitaria, controllo e prevenzione di malattie trasmissibili e per la tutela di gravi minacce per la salute delle persone fisiche.

La seconda eccezione, in particolare, giustifica la presenza di sistemi basati su riconoscimento dei dati biometrici in ambito lavorativo per l’accesso ad “aree critiche”: pensiamo, ad esempio, a quelle zone, all’interno di una grande industria, in cui sono presenti macchinari dall’utilizzo pericoloso per i non addetti ai lavori oppure ai laboratori speciali all’interno degli ospedali, alle torri di controllo e alle aree speciali degli aeroporti o ai caveau delle banche.

Si tratta, in tutti i casi, di zone critiche, il cui ingresso deve essere protetto da un controllo accessi severo e altamente affidabile come quello di tipo biometrico. Che cosa accade, quindi, nel caso in cui si decida di adottare la tecnologia biometrica negli Uffici della Pubblica Amministrazione?

Videosorveglianza e biometria nella Pubblica Amministrazione: il NO del Garante Privacy

La **Legge Concretezza** (19 giugno 2019, n. 56) in tema di “Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell’assenteismo”, aveva previsto, oltre a misure volte a migliorare le capacità e l’efficienza della Pubblica Amministrazione, diversi interventi per la prevenzione dell’assenteismo: impronte digitali a sostituzione del badge e, in più, l’installazione di telecamere di videosorveglianza a varchi di acceso. Più nel dettaglio, la Legge prevede che l’identificazione del dipendente avvenga tramite il riconoscimento delle impronte digitali, controlli dell’iride o riconoscimento vocale, sia in entrata che in uscita.

Chiamato a esprimere il proprio parere sullo schema di decreto riguardante, nello specifico, la prevenzione dell'assenteismo, il **Garante della Privacy ha dichiarato che l'accoppiata rilevazioni biometriche- sistemi di videosorveglianza è "di dubbia compatibilità con le regole della Privacy europea e nazionale"**.

Relativamente all'adozione di telecamere di videosorveglianza per il controllo dei varchi, **manca la proporzionalità tra tale misura e le esigenze organizzativo-produttiv**e, di sicurezza sul lavoro e di tutela del patrimonio aziendale previste dal Provvedimento del Garante della Privacy del 2010, dallo Statuto dei Lavoratori, nonché dalla circolare n. 5/2018 dell'Ispettorato Nazionale del Lavoro.

Riguardo, invece, all'utilizzo di sistemi biometrici, **mancano i presupposti indicati dal GDPR, ovvero fattori di rischio specifici**, la presenza – e il ripetersi – di situazioni critiche, che potrebbero arrecare danno alle persone, all'ambiente e al patrimonio.

Insomma, secondo l'Autorità Garante, **la motivazione "prevenzione dell'assenteismo" non regge, non giustifica la scelte di telecamere e di sistemi biometrici nella Pubblica Amministrazione**. Tale scelta sembra, invece, andare verso il "controllo" del lavoro e dei comportamenti dei lavoratori, tassativamente vietato dalla normativa italiana e internazionale in tema di Privacy.