# Il controllo dei dipendenti alla luce delle ultime interpretazioni

scritto da goal | 14 Novembre 2019

***di Stefano Bacchiocchi****

Il regolamento generale sulla protezione dei dati GDPR non prevede norme specifiche riguardanti il rapporto di lavoro. Ciononostante, i professionisti che si occupano della materia del lavoro ben sanno quanto questa norma abbia impattato non solo sull'organizzazione dello studio ma anche sulle responsabilità (anche penali) che ne derivano.

La normativa è relativamente recente (entrata in vigore solo nel maggio 2018) e quindi si rende necessario un coordinamento costante e non sempre agevole con l'impianto legislativo già esistente; non ultimo lo Statuto dei Lavoratori (L. n. 300/1970) che ha individuato quale principio fondamentale, indipendentemente dal tipo di contratto applicato, il rispetto della vita privata e della dignità del lavoratore.

Sta a noi professionisti, quindi, provare a coordinare il nuovo GDPR con la normativa già presente in materia di lavoro.

In altri articoli su questa stessa rivista, abbiamo già affrontato molti aspetti della normativa privacy; questa volta ci concentreremo sui controlli del lavoratore alla luce delle nuove indicazioni pervenute da più parti in questi mesi.

Come è noto, il GDPR enuncia principi generali, più che elencazioni puntuali; il che rende la normativa estremamente fluida e soggetta ad interpretazioni.

Anche i datori di lavoro quindi dovranno prendere coscienza (se non loro, almeno i loro consulenti) di concetti come:

principio di accountability, principio di proporzionalità ecc. anche nella pianificazione del lavoro e dei controlli interni ed esterni alle aziende.

La tecnologia, in questo senso, è un'arma formidabile ma a doppio taglio, se pensiamo alle nuove modalità di controllo permesse dall'Internet of things, ai GPS, alle smart cam, ai dispositivi indossabili, badge elettronici, lettori di impronte ecc. poiché la facilità di utilizzo e la pervasività dei potenziali controlli mal si coordinano con la normativa privacy vigente; inoltre, la velocità di introduzione di queste tecnologie necessita interpretazioni da parte degli organi istituzionali preposti che non sempre arrivano con celerità.

è quindi chiara la necessita dell'adozione di misure preventive volte alla protezione della riservatezza dei dati dei lavoratori, predisponendo anche delle valutazioni di impatto del trattamento che abbiano ad oggetto il bilanciamento degli interessi in gioco: da un lato, il diritto del datore di lavoro di ottenere una prestazione lavorativa per la quale sta elargendo uno stipendio, dall'altra, il diritto del lavoratore alla dignità, alla libertà personale e, più in generale, alla privacy e protezione dei dati personali.

Ricordo ancora come il GDPR non distingua dal grado di subordinazione o dalla tipologia contrattuale del lavoratore; infatti si rivolge in maniera simile sia ai lavoratori dipendenti sia a quelli autonomi.

Il datore di lavoro può legittimamente porre in essere il controllo dei dipendenti in forza dei diritti e doveri insiti nell'esecuzione di obblighi derivanti da un contratto di lavoro, e, ovviamente, nell'adempimento delle obbligazioni previste nell'interesse legittimo del datore.

Al contrario di quanto il datore di lavoro talvolta si aspetta (spesso il sentire comune non è coerente con quanto previsto

dal GDPR) il consenso non è fonte di liceità del trattamento: quindi a nulla valgono i semplici “accordi” presi tra datore di lavoro e lavoratore.

Anche nel caso i controlli attivati siano legittimi sotto il piano della corrispondenza alle norme di legge, non è detto siano comunque aderenti ai dettati del GDPR: bisogna, infatti, valutare preventivamente la necessità e la proporzionalità del trattamento in essere ed adottare le misure di sicurezza, redigendo, quando obbligatorio, anche una valutazione di impatto del trattamento.

Si ricorda che, in base a questi principi, è imposto al datore di lavoro l’onere di provare anche l’insussistenza di strumenti meno invasivi per il raggiungimento delle finalità del trattamento; in altre parole, non tutto ciò che si può mettere tecnicamente in atto è legittimo e aderente alle prescrizioni del regolamento privacy.

Ad esempio: la possibilità tecnica di rilevare le impronte digitali e gli spostamenti dei dipendenti non è un motivo di per sé sufficiente al fatto di porli in essere, sproporzionato alle finalità e agli scopi prefissati.

Il panorama dei controlli possibili è infinito; proveremo qui a definire alcuni casi tipici al fine di definire le linee guida base per un trattamento corretto.

Un caso tipico sono i dati presenti nei vari social media: il datore di lavoro può trattare i dati dei lavoratori presenti sui loro profili solo quando tali profili siano utilizzati dagli interessati per finalità lavorative e non personali; anche in tale circostanza, il datore di lavoro dovrà informare il lavoratore del trattamento dei suoi dati personali.

Un altro esempio è il trattamento dati personali dei lavoratori relativi all’utilizzo della loro strumentazione informatica (es.: e-mail, telefonate, smartphone ecc.): buone pratiche previste dalle prassi sono la predisposizione di un

elenco di siti in cui la navigazione è vietata, la predisposizione di un apposito regolamento per l'uso della strumentazione ecc.

E' stato dichiarato illegittimo invece il monitoraggio dei movimenti del mouse e l'utilizzo di webcam, in quanto sono eccessive rispetto alle finalità perseguite.

Il controllo degli smartphone sarà sempre più utilizzato a causa dell'utilizzo capillare e personale dei device.

Oramai tutti i principali sistemi operativi permettono al datore di lavoro di gestire da remoto i dispositivi mobili affidati ai lavoratori. In questo caso si consiglia di redigere una DPIA (Data Protection Impact Assessment) prima dell'inizio del trattamento, al fine di verificare la necessità del trattamento rispetto alle finalità perseguite e garantire il rispetto dei principi di proporzionalità e sussidiarietà. Gli strumenti utilizzati dal datore di lavoro al fine di monitorare lo stato di salute e l'attività fisica dei propri lavoratori, spesso anche al di fuori dell'ambiente di lavoro, consentono al datore di raccogliere dati particolari (ex sensibili) degli interessati; potrebbe quindi essere illegittimo fornire ai dipendenti dei device indossabili, che controllino la salute del lavoratore (es. battiti cardiaci ecc.), a meno che i dati raccolti possono essere trattati solo dai diretti interessati e non dal datore di lavoro.

Alcuni strumenti aziendali utilizzati dal datore di lavoro per finalità del tutto legittime possono comportare l'indiretto monitoraggio dei lavoratori nel luogo di lavoro (si pensi, ad esempio, alla rilevazione dei dati biometrici dei lavoratori, per monitorare l'accesso), per poter essere effettuati nel rispetto della normativa vigente, devono essere preceduti da una idonea informativa. Anche in questo caso è opportuno far precedere l'installazione del sistema da una valutazione in merito alla proporzionalità di tale implementazione: potrebbe

essere illegittimo l’utilizzo dei dati biometrici, in sostituzione del semplice badge aziendale, per quei lavoratori che non trattano dati particolari in aree sensibili.

L’utilizzo delle tecnologie che consentono il video monitoraggio dei lavoratori (es.: monitoraggio facciale mediante la videocamera dello smartphone affidato ai lavoratori) è illecito, in quanto sproporzionato rispetto alla tutela dei diritti e delle libertà fondamentali degli interessati.

In particolare, sulla videosorveglianza è intervenuta recentemente una sentenza della Grande Camera della Corte di Strasburgo che giustifica in parte, l’utilizzo di telecamere nascoste; si conferma però l’utilizzo del principio di proporzionalità come requisito essenziale.

Le telecamere nascoste sul luogo di lavoro, quindi, possono essere utilizzate quando ricorrano determinati presupposti: ad esempio, quando esistano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale; l’area oggetto di ripresa sia circoscritta; le videocamere siano in funzione per un periodo temporale limitato; quando non sia possibile ricorrere a mezzi alternativi; quando le immagini captate siano utilizzate soltanto a fini di prova dei furti commessi (si consiglia di coordinarsi anche con le autorità preposte). La videosorveglianza occulta è, dunque, ammessa solo a fronte di gravi fatti illeciti e non può diventare una prassi.

Un altro tema molto in voga nel settore della logistica, ma non solo, è la geolocalizzazione dei veicoli: se è effettuata al solo fine di monitorare il comportamento dei lavoratori, è illecita; se il trattamento è effettuato invece per il perseguimento di finalità legittime, ad esempio la tutela della sicurezza dei veicoli o per la pianificazione delle attività lavorative, risulta lecito.

In ogni caso, si suggerisce di evidenziare all'interno dei veicoli una informativa privacy che avvisi dell'utilizzo del sistema di geolocalizzazione; si consiglia comunque di effettuare una analisi preventiva che preveda la possibilità di disattivare il sistema nei casi in cui il veicolo sia utilizzato per finalità private.

Come visto, le nuove tecnologie avanzano velocemente e talvolta il confine tra pianificazione delle attività, tutela del patrimonio e controllo illegittimo è sempre più sottile.

Le sanzioni anche in questo caso sono importanti e prevedono l'applicazione di più normative: della sicurezza sul lavoro, della tutela del patrimonio, dei rapporti di lavoro, sulla privacy, sulla protezione e la sicurezza dei dati ecc., è opportuno quindi confrontarsi con professionisti esperti e non affidarsi ciecamente agli installatori che potrebbero non avere le competenze necessarie (né l'interesse) a gestire questo tipo di fenomeni. Inoltre, poiché solitamente i primi a conoscere l'implementazione di questi strumenti sono proprio i nostri studi professionali, c'è la necessità di porre in essere i corretti adempimenti tempestivamente e con competenza.

Consiglio, quindi, eventualmente di attivare delle consulenze specifiche con esperti del settore (es. consigliare la nomina di un DPO), al fine di scongiurare sanzioni, eccessiva burocratizzazione e danni sia a carico del cliente sia dei nostri studi professionali.

**Odcec Brescia*