

Videosorveglianza

## La gestione del personale di società partecipate “tra pubblico e privato”: bilanciamento tra potere datoriale e diritto alla privacy del lavoratore

di Iacopo Cavallini e Maria Orsetti - Dipartimento di Economia e Management, Università di Pisa

Uno dei temi di maggior attualità in questi anni è quello dell'individuazione, nell'ambito dell'instaurazione e gestione dei rapporti di lavoro dipendente delle società partecipate dalla PA, del perimetro all'interno del quale trova applicazione la legislazione speciale “pubblica”.

Venuto meno ogni dubbio in ordine all'applicabilità del Testo Unico sul Pubblico Impiego (D.Lgs. n. 165/2001) nella gestione del personale dipendente delle partecipate, e sancita la loro riconducibilità al diritto privato, l'elaborato affronta come il contemperamento tra quest'ultimo e la normativa sulla *Privacy* può riflettersi sui rapporti tra datore di lavoro e dipendenti. Si analizza, a tal fine, un caso di estrema attualità.

### **La cornice normativa di riferimento per la gestione dei rapporti di lavoro dipendente nelle società a partecipazione pubblica, e la sua evoluzione**

Uno dei temi di maggior attualità in questi anni è quello dell'individuazione, nell'ambito dell'instaurazione e gestione dei rapporti di lavoro dipendente delle società partecipate dalla PA, del perimetro all'interno del quale trova applicazione la legislazione speciale “pubblica”.

Da questo punto di vista, il Legislatore con il D.Lgs. n. 175/2016 ha finalmente stabilito dei punti fermi colmando quel vuoto normativo che si era venuto a creare nel passato, e su cui la giurisprudenza ha maturato orientamenti interpretativi troppo spesso contrastanti.

Gli aspetti intorno ai quali l'incertezza si è manifestata in misura più rilevante sono riconducibili essenzialmente alle modalità di assunzione (con i connessi

effetti sulla validità dei rapporti di lavoro sorti senza il previo esperimento di procedure a evidenza pubblica), alla giurisdizione del Giudice Ordinario in alternativa a quello Amministrativo e, infine, alla legislazione applicabile ai rapporti di lavoro già costituiti.

Il D.Lgs. n. 175/2016, all'art. 19, ha chiarito ognuno di questi dubbi stabilendo che:

- l'obbligo di effettuare selezioni pubbliche in conformità al disposto di cui all'art. 35, comma 3, D.Lgs. n. 165/2001, con riferimento alle sole società in controllo pubblico, è condizione necessaria ai fini della validità dei rapporti di lavoro che se diversamente instaurati sono nulli;
- che tutte le questioni attinenti alla tematica del personale dipendente ricadono nella giurisdizione del Giudice Ordinario;
- e, infine, che i rapporti di lavoro, una volta costituiti, sono assoggettati esclusivamente alla

normativa di diritto comune e quindi al CCNL operante e allo Statuto dei diritti dei lavoratori (Legge 20 maggio 1970, n. 300).

## **Il contemperamento tra potere datoriale e diritto alla *privacy* del lavoratore: l'utilizzo di riprese video attraverso telecamere nascoste**

Venuto meno ogni dubbio in ordine all'applicabilità del Testo Unico sul Pubblico Impiego (D.Lgs. n. 165/2001) nella gestione dei rapporti di lavoro dipendente delle partecipate, e sancita la loro riconducibilità al diritto privato, si tratta ora di accertare in che modo la normativa sulla *privacy* possa incidere su di essa affrontando un caso di estrema attualità.

“Un datore di lavoro può installare delle telecamere nascoste senza informare i dipendenti se ha il fondato sospetto che questi lo stiano derubando e se le perdite subite per la loro condotta sono ingenti”: questo ha stabilito la *Grand Chamber* della Corte Europea dei Diritti dell'Uomo (CEDU), con sentenza del 17 ottobre 2019 sui ricorsi n. 1874/13 e n. 8567/13 - López Ribalda e altri *versus* Spagna.

La sentenza che, a una lettura poco approfondita, potrebbe condurre ad abnormi interpretazioni lesive dei diritti sulla *privacy* dei lavoratori, deve essere invece attentamente analizzata alla luce del Regolamento Ue 2016/679, noto come GDPR (*General Data Protection Regulation*), della normativa nazionale di recepimento (D.Lgs. 10 agosto 2018, n. 101), e del D.Lgs. 14 settembre 2015, n. 151 (*Jobs Act*), che ha riscritto l'art. 4 dello Statuto dei diritti dei lavoratori; ciò al fine di evitare di estenderne, attraverso frettolose interpretazioni, la portata applicativa.

La pronuncia, infatti, è strettamente collegata e motivata in relazione alla fattispecie concreta, alle modalità con cui si sono svolti i fatti e alle condotte del datore di lavoro e dei lavoratori. Per questo si rende particolarmente utile esaminare la vicenda specifica. Il caso all'origine della pronuncia risale al 2009, dunque a un periodo antecedente all'emanazione del GDPR, quando il direttore di un supermercato spagnolo in provincia di Barcellona ha rilevato irregolarità tra *stock* di magazzino e vendite, oltre a una rilevante perdita negli incassi nell'arco di cinque mesi (circa 82 mila euro). Non solo: i furti iniziati per poche migliaia di euro erano, di mese in mese, in costante crescita. Inoltre, era stato verificato con ragionevole certezza che gli illeciti fossero commessi da dipendenti e non da clienti o da altri soggetti terzi. La Direzione era giunta a tale conclusione poiché dall'esame della documentazione elettronica, ossia

gli scontrini, aveva constatato che molti di essi venivano annullati dopo che era stato letto il codice a barre, mentre le merci non venivano restituite (e quindi non si trovavano più all'interno dell'esercizio commerciale), oppure per errori di battitura relativamente a somme di cui poi non vi era esistenza di cassa.

Insospettito da tali circostanze, il *manager* del supermercato ha quindi deciso di far installare alcune telecamere a circuito chiuso, sia visibili (alle uscite) sia - previo accordo sindacale e notifica alle autorità competenti, in linea con la normativa spagnola allora vigente - nascoste (puntate sulle casse). Dunque, la raccolta dei dati personali era avvenuta secondo le regole.

Successivamente le videoriprese hanno confermato una serie di furti di merci e di denaro da parte del personale e, per questo, sono state fatte visionare agli interessati affinché potessero esercitare il loro diritto alla difesa. Ai lavoratori è stato dunque consentito di contestare l'utilizzo della ripresa come mezzo di prova, o perché illegittimamente utilizzato a fini disciplinari in quanto riprodotto senza il loro consenso, o perché non veritiero, o più in generale perché lesivo del diritto alla *privacy*.

I dipendenti, invece, hanno ammesso i furti, denunciandosi a vicenda, e si sono difesi sul contenuto dei video, di fatto acconsentendo, con tale condotta, al loro uso come mezzo di prova: essendo, la riservatezza, un diritto assolutamente disponibile. Inoltre, riconoscendo gli illeciti hanno generato ulteriori elementi di prova, di natura testimoniale.

Per questo insieme di motivi, i lavoratori sono stati licenziati. Dopo aver presentato ricorso avverso al provvedimento di fronte al Giudice del Lavoro spagnolo, che ha confermato la legittimità del provvedimento disciplinare espulsivo, si sono rivolti alla Corte d'appello della Catalogna. Quest'ultima ha ribadito la correttezza dell'installazione delle videocamere, in considerazione del fatto che erano già presenti elementi oggettivi e documentali riguardanti i furti: era stato accertato, infatti, che gli illeciti avvenivano ormai da diversi mesi e che erano commessi da dipendenti. Il presupposto dell'esistenza di un furto da parte di dipendenti veniva ritenuto così grave da giustificare il ricorso a un mezzo di accertamento estremo, quale la videocamera nascosta.

Nonostante i licenziamenti siano stati considerati legittimi dai tribunali nazionali, cinque dei dipendenti allontanati hanno deciso di ricorrere alla Corte di Strasburgo, sostenendo che, in base al diritto spagnolo, i cassieri avrebbero dovuto essere informati

preventivamente della sorveglianza e che, pertanto, l'utilizzo delle videoriprese come mezzo di prova era lesivo del loro diritto alla *privacy*.

Nel ricorso si chiedeva, quindi, di censurare le conclusioni della giustizia spagnola riconoscendo in particolare una violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo sul diritto al rispetto della vita privata e familiare.

Secondo la Corte di Giustizia Europea (CEDU) i giudici spagnoli hanno "attentamente bilanciato" i diritti contrapposti dei lavoratori e del datore di lavoro, effettuando un'analisi specifica delle ragioni che hanno indotto quest'ultimo a collocare le videocamere nascoste. E la mancata preventiva notifica su alcune delle telecamere presenti nell'esercizio risulta giustificata dal ragionevole sospetto, quasi certezza, di condotte illecite dei dipendenti e dall'ingente perdita economica.

La Corte di Giustizia adita ha stabilito, inoltre, che non vi è stato un illegittimo utilizzo della videosorveglianza, poiché i lavoratori avevano avuto accesso alle riprese fin dalla contestazione disciplinare e, quindi, erano stati messi in condizione di poter esercitare il proprio diritto alla difesa. Nel ritenere la ripresa proporzionata e legittima, e la lesione della *privacy* non sproporzionata, fattore decisivo è stata anche la sua breve durata (10 giorni) e il numero limitato delle persone messe a conoscenza dei video; le riprese, infatti, sono state utilizzate solo per fini processuali ed esibite esclusivamente alla magistratura come mezzi di prova, e non diversamente diffusi a terzi.

Decisiva anche la scarsa estensione dell'area sorvegliata, limitata alla zona casse. Inoltre le telecamere, seppure nascoste, erano poste in un luogo aperto al pubblico, dove si maneggiavano denaro o merci. Infine, i lavoratori, con una procedura in linea con la normativa spagnola a quel tempo vigente, erano comunque stati messi a conoscenza che i locali erano video sorvegliati.

Per la CEDU, il livello di *privacy* che un dipendente può legittimamente attendersi dipende, infatti, anche dalla posizione fisica dei locali: molto elevato in luoghi privati (servizi igienici o guardaroba), dove vi è un divieto assoluto di videosorveglianza; elevato in spazi di lavoro ristretti (uffici), dove può essere giustificato; inferiore, negli spazi di lavoro visibili o accessibili ai colleghi o al pubblico in generale.

I diritti fondamentali dei lavoratori, dunque, secondo la CEDU - che non può entrare nel merito del corretto operare delle giurisdizioni nazionali per

aspetti diversi dalla tutela dei diritti umani - sono stati rispettati.

La decisione in esame statuisce che i provvedimenti nazionali non sono sindacabili perché sono stati salvaguardati, nel caso concreto, i diritti fondamentali dell'uomo, quali la *privacy* e il diritto di difesa. L'opinione dissenziente da parte di tre giudici della Corte di Strasburgo che, secondo il diritto comunitario, viene annotata nel provvedimento, fornisce spunti interessanti per alcune riflessioni.

Secondo questa tesi, a nostro giudizio condivisibile, il caso rischia di creare un pericoloso precedente di apertura all'ingerenza nella vita quotidiana delle persone che, grazie agli sviluppi tecnologici (sempre più ingenti moli di dati archiviabili, costi sempre meno elevati della tecnologia, ecc.), può raggiungere livelli incontrollabili, astrattamente fino al punto di consentire di poter archiviare l'intera vita di una persona.

Rispetto alla citata sentenza della CEDU, il Garante italiano della *privacy* nel comunicato del 17 ottobre 2019 ha precisato che "La sentenza della Grande Camera della Corte di Strasburgo se da una parte giustifica, nel caso di specie, le telecamere nascoste, dall'altra conferma però il principio di proporzionalità come requisito essenziale di legittimazione dei controlli in ambito lavorativo". Per dichiarare legittimo l'uso di una videosorveglianza occulta su di un luogo di lavoro è stato accertato che ricorrevano specifiche e peculiari circostanze: "... vi erano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale, l'area oggetto di ripresa (peraltro aperta al pubblico) era alquanto circoscritta, le videocamere erano state in funzione per un periodo temporale limitato, non era possibile ricorrere a mezzi alternativi e le immagini captate erano state utilizzate soltanto a fini di prova dei furti commessi".

Secondo il Garante, dunque, la sentenza in esame conferma quanto stabilito dalla normativa nazionale in tema di controlli a distanza sui luoghi di lavoro, ovvero che "la videosorveglianza occulta è ammessa solo in quanto *extrema ratio*, a fronte di "gravi illeciti" e con modalità spazio-temporali tali da limitare al massimo l'incidenza del controllo sul lavoratore. Non può dunque diventare una prassi ordinaria. Il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque, la loro rigorosa proporzionalità e non eccedenza: capisaldi della disciplina di protezione dati".

## **Una possibile chiave di lettura per il prudente bilanciamento tra diritto alla riservatezza e rischio aziendale di incorrere in conseguenze rilevanti**

In altre parole, il Garante sostiene che la sentenza della CEDU è strettamente motivata in relazione al caso concreto, e non può diventare l'argomentazione per installare come prassi ordinaria un sistema di videoriprese occulte.

In tutta onestà, ci pare che il Garante non abbia assunto una posizione netta, e che le sue affermazioni siano poco risolutive. Per l'esame dei casi concreti servirebbero, infatti, parametri di riferimento, a meno che lo stesso Garante non abbia inteso di fare propri, condividendoli, gli orientamenti della giurisprudenza formati nel corso dell'ultimo decennio.

Il rischio di "abuso" sotteso all'utilizzo di telecamere nascoste appare molto elevato, e una chiave di lettura estensiva della posizione della CEDU potrebbe aprire la strada ad analoghi rischi per altre fattispecie di raccolta, trattamento e utilizzo di dati e informazioni personali.

Ci riferiamo ad "abusi" che devono essere scongiurati ma che, a ben vedere, la giurisprudenza già riconosce e tende a reprimere con forza, viste le posizioni particolarmente stringenti assunte in Italia.

Ove infatti non sia rispettata la procedura prevista dallo Statuto dei diritti dei lavoratori (art. 4) per l'installazione delle telecamere, anche non occulte, i dati sono da considerarsi illegittimamente acquisiti e non utilizzabili, in quanto illegittimo sarebbe il loro trattamento, e il Datore di

lavoro, conseguentemente, commetterebbe un reato. Da questo punto di vista non è sufficiente il consenso eventualmente espresso direttamente dai dipendenti, e non per il tramite delle rappresentanze sindacali o previa autorizzazione della Direzione Territoriale del Lavoro.

La Corte Suprema di Cassazione, sez. III pen., nella sentenza n. 38882/2018 a questo proposito ha stabilito che l'eventuale consenso rilasciato direttamente dai lavoratori non è, per il datore di lavoro, una discriminante rispetto al reato di cui all'art. 4, Legge n. 300/1970, in quanto in assenza di un accordo con i sindacati o con la DTL viene a mancare un controllo sulla legittimità dell'installazione del sistema di videosorveglianza.

Si tratta, in altri termini, del mancato coinvolgimento di soggetti competenti e dotati di una maggiore forza economico-sociale rispetto ai singoli dipendenti, i quali nel rapporto di lavoro rappresentano una controparte debole e facilmente condizionabile.

Dato atto che il D.Lgs. n. 175/2016 ha fugato ogni incertezza circa la riconducibilità del rapporto di lavoro nelle società controllate o semplicemente partecipate dalla PA al diritto comune, e che non esistono nell'ordinamento disposizioni analoghe a quelle contenute nel Testo Unico sul Pubblico Impiego, appare dunque evidente che il "pubblico", quando opta per operare attraverso società di capitali, non potrà che far ricorso - alla stregua di qualsiasi imprenditore privato - agli strumenti che lo stesso diritto comune mette a disposizione per contemperare le diverse esigenze delle parti coinvolte.