LABOR Il lavoro nel diritto

Pacini Giuridica

Utilizzabilità delle registrazioni video effettuate nei luoghi di lavoro come fonte di prova di illeciti disciplinari

di R. Maurelli - *31 Maggio 2023*

Con l'ordinanza n. 8375 del 23 marzo 2023, qui annotata, la Cassazione è tornata ad occuparsi dell'utilizzabilità delle registrazioni video come fonte di prova di illeciti disciplinari del dipendente.

Il caso di specie riguardava una festa di fine anno scolastico, divenuta teatro di un episodio di scontro fra un gruppo di studenti ed un educatore professionale. Quest'ultimo, infatti, aveva punito i ragazzi, ordinandogli di rientrare anticipatamente, ma questi ultimi si erano opposti, tenendo un comportamento provocatorio; a fronte di ciò l'insegnante aveva afferrato uno di loro per la maglietta, accompagnandolo con forza verso l'ascensore e, nello spingerlo, lo aveva fatto cadere per terra.

La scena, interamente registrata dal sistema di videosorveglianza della scuola, era stata, poi, posta a base della sanzione disciplinare della sospensione dell'insegnante dal servizio e della retribuzione.

Nel giudizio di Cassazione, il lavoratore aveva lamentato, fra l'altro, un vizio di motivazione della sentenza di appello riguardante l'inutilizzabilità a fini disciplinari delle riprese effettuate dal sistema di videosorveglianza.

La Suprema Corte ha però rigettato la censura, rilevando che la Corte di Appello aveva compitamente argomentato sulle ragioni di utilizzabilità delle suddette riprese, accertando che l'impianto di registrazione era destinato ad esigenze di sicurezza sul lavoro e installato previo accordo sindacale, nel rispetto delle prescrizioni dell'art. 4 Stat. lav., nella versione anteriore alle modifiche apportate dal D.lgs. n. 151/15.

A prescindere dalla decisione del caso concreto, la suddetta statuizione induce a domandarsi, su un piano più generale e alla luce della disciplina oggi vigente, se l'utilizzabilità delle registrazioni video sia effettivamente lecita, in presenza dei due soli requisiti della finalità di sicurezza sul lavoro e dell'autorizzazione sindacale, espressamente prescritti ai fini dell' «*impiego*» dello strumento di controllo, ancora prima che per l'utilizzabilità stessa.

A questa domanda il legislatore del 2015 aveva risposto introducendo nel nuovo art. 4, comma 3, Stat. lav. due espresse condizioni di utilizzabilità delle informazioni raccolte: da un lato, l' «*adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*», dall'altro, il rispetto del codice della privacy. Il rispetto di tali due condizioni, dunque, è necessario e non può che aggiungersi ai requisiti per l'impiego dello strumento di cui al comma 1.

Occorre allora chiedersi quale sia l'esatto contenuto di questi oneri di cui è gravato il datore di lavoro, al fine di comprendere quando i dati acquisiti sono «*utilizzabili a tutti i fini connessi al rapporto di lavoro*», compresi quelli disciplinari, e quando, invece, non lo sono.

Sembra ormai essere questo, infatti, il terreno su cui si giocherà la partita dell'utilizzabilità, destinata, prima o poi, a diventare il tema principale della nuova elaborazione giurisprudenziale sui controlli datoriali.

Il primo profilo problematico riguarda il livello di dettaglio dell'informativa, che, come si è detto, viene genericamente descritta come «*adeguata*».

Il concetto di adeguatezza può essere ragionevolmente declinato nelle tre dimensioni della chiarezza, comprensibilità e completezza.

A tal fine, pur non essendo espressamente richiesto dalla norma alcun requisito formale, sembra quantomeno opportuno che l'informativa sia redatta in forma scritta, in modo da non lasciare adito a dubbi circa il suo contenuto.

Inoltre sembra coerente con la *ratio* della norma che la suddetta informazione debba essere anche fornita preventivamente al lavoratore. Indicazioni sistematiche al riguardo possono rinvenirsi nell'ormai abrogato art. 13 del D.lgs. n. 196/2003, il quale precisava che l'informazione deve essere offerta «*previamente*», nonché negli artt. 12 e ss. del GDPR.

Sembra altresì opportuno che l'informativa sia mirata, e non generalizzata a tutti i dipendenti dell'azienda e a tutti i vari strumenti variamente impiegati da ciascuno di essi, perché altrimenti potrebbe essere minata la puntuale conoscenza di quali sono, in concreto, i controlli a cui ciascun lavoratore è assoggettato. Potrebbe, tuttavia, darsi il caso che tutti i dipendenti siano oggetto del medesimo tipo di controllo e da parte dei medesimi dispositivi; in tal caso, evidentemente, si potrà valutare l'opzione di un'informativa generalizzata, ad esempio mediante affissione nella bacheca aziendale o pubblicazione sul sito intranet aziendale.

L'informativa, poi, dovrà essere concisa, non potendosi trasformare in quello che è stato definito "un manualetto di istruzioni" sul funzionamento generale del dispositivo, poiché l'eccessiva mole di dettagli potrebbe inficiare la chiarezza e comprensione, rendendo sostanzialmente impossibile l'esercizio dei propri diritti. Pertanto, si dovranno identificare le sole modalità di utilizzo del dispositivo e di effettuazione dei controlli che hanno un riflesso, anche indiretto, sul diritto alla riservatezza del dipendente, comportando l'acquisizione di dati relativi alla sua attività, In sostanza, occorre spiegare in modo puntuale come le funzionalità dello strumento si raccordano con il sistema dei controlli, il loro scopo, la tempistica degli stessi, la tipologia di dati raccolti, la loro collocazione in azienda (ove si tratti di strumenti fissi), ma niente di più.

Naturalmente una certa variabilità nel livello di approfondimento dell'informativa è inevitabile, poiché dipende dal singolo contesto aziendale e dal grado di rischio per la riservatezza connesso al tipo di sorveglianza messo in atto. Tanto è vero che vi sono stati casi in cui è stata ritenuta sufficiente perfino un'informativa redatta anteriormente all'entrata in vigore della riforma, in quanto già completa di tutti i requisiti minimi da essa dettati (Cass. 24 febbraio 2020, n. 4871, in *RFI*, voce Lavoro (rapporto), 2020, 1400).

L'altro limite all'utilizzabilità delle informazioni raccolte è costituito, poi, dal rispetto della disciplina in tema di privacy, che contiene al suo interno una lunga serie di prescrizioni, e non soltanto quella in tema di liceità, che può ritenersi già assolta mediante il rispetto delle previsioni dell'art. 4 Stat. lav.

Invero, accanto, alla liceità, figura altresì il principio di limitazione della finalità, che costituisce una sorta di precondizione per l'attuazione degli altri princípi, in quanto implica che l'utilizzabilità dei dati sia legittima solo se è coerente con il fine del trattamento stesso indicato dal datore di lavoro nell'informativa.

Da questo principio discendono gli altri corollari, e cioè:

1. che vengano acquisite solo le informazioni strettamente necessarie alle suddette esigenze e che esse vengano trattate da un numero il più possibile ristretto di soggetti (c.d. principio di minimizzazione);

2. che il dispositivo sia impostato in modo tale che i dati siano automaticamente cancellati una volta che non risultino più indispensabili allo scopo prefissato o che siano già stati trattati dal datore di lavoro (principio della limitazione della conservazione dei dati);

3. che datore di lavoro adotti tutte le misure necessarie per assicurare la sicurezza dei dati raccolti, impedendone l'accesso a soggetti non autorizzati (princípi di integrità e riservatezza dei dati).

Sul punto, si è pronunciata anche la Corte Europea dei Diritti dell'Uomo (European Court of Human Rights (Grand Chamber), case of Bărbulescu v. Romania, Application n., 61496/08, 5 September 2017), in un caso in cui un lavoratore eccepiva l'illegittimità del licenziamento per inutilizzabilità dei dati raccolti.

La Grande Camera di Strasburgo, in tale occasione, ha individuato espressamente i criteri che devono guidare i giudici nazionali nel valutare se una determinata misura di controllo sia proporzionata all'obiettivo perseguito e se il dipendente sia tutelato contro interferenze arbitrarie nella sua sfera personale. A tal fine, dunque, i giudici dovranno valutare:

1. se il dipendente è stato informato della possibilità che il datore di lavoro monitori la sua attività;

2. se il dipendente è stato informato della modalità con cui vengono attuate tali misure;

3. quale sia l'estensione del controllo da parte del datore di lavoro e il grado di intrusione nella privacy del dipendente;

4. se il datore di lavoro abbia fornito motivazioni legittime per giustificare il monitoraggio;

5. se sia possibile istituire un sistema di monitoraggio basato su metodi e misure meno intrusivi;

6. quali siano le conseguenze del monitoraggio per il lavoratore subordinato e quale l'uso da parte del datore di lavoro dei risultati dell'operazione di monitoraggio;

7. se siano state predisposte adeguate misure di salvaguardia in favore del lavoratore.

Il grande tema del rispetto della disciplina privacy pone, poi, ulteriori oneri a carico del datore di lavoro, che spesso, ed incredibilmente, vengono del tutto ignorati, come se il GDPR non fosse mai entrato in vigore e non avesse ridisegnato, come in effetti è accaduto, l'intera disciplina sulla tutela dei dati personali.

Ci si riferisce, in primo luogo, alla necessità di effettuare una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento, laddove il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, «*allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità […]*».

Tali trattamenti si considerano a «*rischio elevato*» se presentano nove caratteristiche elaborate dal Gruppo Di Lavoro Articolo 29 per la Protezione dei Dati, e cioè: 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o dati aventi carattere altamente personale; 5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combinazione di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9) ostacolo all'esercizio di un diritto ovvero all'avvalersi di un servizio o di un contratto".

Alla luce delle suddette nonve caratteristiche il Garante privacy, con provvedimento dell'11 ottobre 2018, ha elaborato un "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" e, fra queste tipologie di trattamenti, ha espressamente annoverato anche il trattamento svolto «*nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti*».

Pertanto, alla luce di quanto sopra esposto, sembra ineludibile la necessità di effettuare una valutazione d'impatto sulla protezione dei dati da parte del datore di lavoro.

Più controverso è se il datore di lavoro debba adempiere l'altro pregnante onere, anch'esso non sempre adeguatamente valorizzato, di acquisire il consenso del lavoratore.

Sul punto vi sono opinioni divergenti tra chi ritiene sufficiente la sola informativa ai sensi dell'art. 4, comma 3, Stat. lav., e chi, invece, assume la necessità dell'espresso consenso del lavoratore in aggiunta ad essa.

Tuttavia, volendo ragionare in punto di stretto diritto, sembra che il controllo tecnologico trovi la sua base giuridica nell'art. 6, par. 1, lett. f), del regolamento europeo, in tema di c.d. interesse del titolare, del quale l'art. 4 Stat. lav. costituisce applicazione restrittiva ai sensi dell'art. 88, par. 2, del regolamento medesimo. Pertanto, sembra possibile sostenere che la disciplina dell'informativa di cui all'art. 4, comma 3, Stat. lav. goda di una sua particolare autonomia,

che sarebbe incompatibile con il ripristino di un obbligo di consenso in forza della più generale disciplina europea.

Ovviamente ciò non significa la liberalizzazione assoluta dell'utilizzo di tutti i tipi di dati, poiché i dati personali c.d. sensibili richiedono pur sempre il consenso esplicito (cfr. art. 9, GDPR), e, in taluni casi (ad es. opinioni politiche, religiose e sindacali) sono addirittura radicalmente vietati *ex* art. 8 Stat. lav., anche a prescindere da un eventuale consenso del lavoratore.

Ancora, sembra potersi escludere la necessarietà del consenso in tutti i casi in cui il rapporto di lavoro sia caratterizzato da un «*evidente squilibrio tra l'interessato e il titolare del trattamento*», poiché in tal caso il consenso non potrebbe costituire una valida base giuridica per un trattamento di dati cui è «*improbabile che il consenso sia stato prestato liberamente*» (Considerando n. 43 GDPR).

Se, infatti, è vero che il Regolamento consente il trattamento dei dati «*nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione*» e «*esecuzione del contratto di lavoro*», è anche vero, dall'altro lato, che, al di fuori da questi compiti specificamente elencati, si dovrebbe ritenere che il consenso rientri nell'ipotesi di squilibrio contemplata nel preambolo ogni volta che il trattamento dei dati non sia assolutamente e strettamente reso necessario dall'adempimento amministrativo, contabile, fiscale o contributivo connesso al rapporto di lavoro. Infatti, il Regolamento precisa che «*si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso*»(Considerando n. 43 GDPR).

Resta il fatto che, in questa situazione di incertezza, sarebbe comunque preferibile acquisire anche il consenso del lavoratore, tantopiù che esso potrà essere raccolto all'interno della medesima informativa redatta ai sensi dell'art. 4, comma 3, Stat. lav.

Roberto Maurelli, avvocato in Roma e dottore di ricerca

Visualizza il documento: Cass., ordinanza 23 marzo 2023, n. 8375