LABOR Il lavoro nel diritto

Pacini Giuridica

Videosorveglianza del lavoratore a tutela del patrimonio aziendale e prove digitali

di C. Ogriseg - *28 gennaio 2025*

L'ordinanza 6 settembre 2024, n. 23985 della Corte di Cassazione, qui commentata, esamina la legittimità di un licenziamento disciplinare, intimato grazie a videoriprese delle attività in una biglietteria. Il sistema di videosorveglianza filmava un addetto alla biglietteria che non consegnava ai clienti il resto dovuto, senza registrare l'esubero di cassa; sicché l'azienda procedeva con la contestazione del comportamento e il successivo licenziamento.

La Corte di appello, in riforma della pronuncia di primo grado emessa nell'ambito di un procedimento *ex* lege n.92/2012, dichiarava la legittimità del licenziamento. I Giudici di secondo grado, presa visione del filmato, accertavano che le operazioni di cassa registrate erano state pienamente corrispondenti a quanto addebitato nella lettera di contestazione e idonee a ledere irrimediabilmente il vincolo fiduciario poiché le mansioni in concreto rivestite comportavano maneggio di denaro.

Quanto all'impianto di videosorveglianza i Giudici ne evidenziavano la legittimità e il rispetto della dignità e della riservatezza dei dipendenti.

L'impianto audiovisivo di controllo era stato installato, previo accordo sindacale: le telecamere erano state posizionate, in maniera tale da riprendere solo lo scambio di denaro, senza inquadrare l'addetto alla cassa, con la dichiarata finalità di tutela del patrimonio aziendale e la salvaguardia delle esigenze di sicurezza; infine, le videoriprese avrebbero potuto essere visionate solo in caso di reclamo della clientela. Le censure di autenticità del dato informatico, estratto dal sistema di videosorveglianza e dedotto in giudizio dalla società, venivano rigettate poiché generiche e non circostanziate.

L'addetto alla biglietteria impugna la sentenza della Corte di Appello e presenta ricorso in Cassazione.

Oppone innanzitutto che le immagini erano state visionate senza che fosse stato presentato reclamo da parte della clientela (come richiesto dall'accordo collettivo aziendale).

In secondo luogo, oppone che le videoriprese erano state acquisite in violazione dei principi contenuti nella legge n.48/2008 e art.2712 c.c. poiché l'estrazione di copia dei filmati del servizio di videosorveglianza era stata effettuata senza che fosse stata garantita l'integrità e la genuinità delle immagini registrate.

In terzo luogo, oppone che i dati informatici prodotti in giudizio erano inutilizzabili poiché non erano stati realizzati in una copia forense e infine che il sistema di videosorveglianza non era "a norma" poiché le immagini erano state conservate oltre il termine di 7 giorni previsto nell'accordo sindacale.

Nell'ordinanza in esame la Corte di Cassazione osserva, innanzitutto, come la fattispecie sia estranea alla tematica dei cd. controlli difensivi in senso stretto e trovi applicazione l'art.4 co.1, legge n.300/1970 così come modificato dall'art.23 d. lgs. n.151/2015. La norma consente l'installazione di impianti di videosorveglianza da cui *"derivi anche la possibilità di*

controllo a distanza dell'attività dei lavoratori" previo accordo collettivo, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

In altri termini, la fattispecie rientra tra i controlli a difesa del patrimonio aziendale e le questioni attengono all'utilizzabilità delle informazioni raccolte.

La ricostruzione degli ermellini risulta condivisibile. L'installazione di un impianto di videosorveglianza, dal quale derivi – anche – la possibilità di controllo a distanza dell'attività dei lavoratori è lecita in presenza di accordo collettivo sottoscritto con le organizzazioni sindacali. Sul punto e per approfondimenti si segnalano M. P. MONACO, "*Controlli a distanza sui lavoratori: evoluzione, riforme e privacy*" in *Labor, Fascicolo 2/2021* e D. SERRA, *Sulla legittimità dei controlli difensivi del datore di lavoro pubblico in un caso di accesso abusivo alla banca dati dell'ente,* in *www.rivistalabor.it, 9 maggio 2024.*

Nella fattispecie esaminata, l'installazione dell'impianto è pacificamente autorizzata con la sottoscrizione dell'accordo sindacale.

Ciò che non risulta oggetto di valutazione è, invece, il ben più importante profilo dell'adeguatezza dell'informativa sul trattamento dei dati personali, presupposto di "utilizzabilità" delle videoriprese (cfr. art.13 Reg. UE n.2016/679 e art.4 l.n.300/1970). In effetti, la Corte rileva come la difesa non abbia formulato contestazione alcuna riguardo l'adeguatezza dell'informazione ai dipendenti in merito alle modalità d'uso degli strumenti e all'effettuazione dei controlli.

Nella parte motiva dell'ordinanza si evidenzia come il ricorrente si sia limitato ad opporre che nell'accordo sindacale era previsto che l'identificazione degli addetti alla cassa sarebbe avvenuta solo in presenza di dettagliato reclamo della clientela, senza contestare una non completa informazione sul trattamento dei dati personali. E si precisa altresì come anche tale censura sia irrilevante.

Ai sensi dell'accordo sindacale, il reclamo della clientela sarebbe stato necessario solo qualora la finalità della visione delle immagini fosse stata diversa da quella di "tutela del patrimonio aziendale".

Tuttavia, nel caso di specie la verifica delle riprese era stata correttamente eseguita nell'esigenza di protezione del "patrimonio aziendale" in una accezione estesa. La Corte richiama i propri precedenti in cui si conferma che "*il diritto del datore di lavoro di tutelare il proprio patrimonio, […] costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico"* (cfr. Cass. n.2722/2012).

Ritiene dunque la Suprema Corte che la tutela del patrimonio aziendale ben possa riguardare la difesa datoriale da condotte di appropriazione di denaro e di danneggiamento o sottrazione di beni, le quali possono provenire anche da dipendenti dell'azienda e che giustificano la medesima protezione rispetto a quelle dovuta a fronte di condotte esterne.

Al riguardo, osserva come la tutela debba riguardare sia le lesioni all'immagine, sia al patrimonio reputazionale dell'azienda, né sia dubitabile che eventuali condotte fraudolente di dipendenti in danno di clienti siano del pari idonee a pregiudicare l'immagine di una impresa.

Pertanto, lo strumento tecnologico che aveva permesso la videoripresa della biglietteria nel caso di specie risultava pacificamente installato in modalità non occulte e non concretanti un mero controllo sull'eventuale inadempimento nell'esecuzione della prestazione lavorativa da parte dei lavoratori.

Le argomentazioni utilizzate sono conformi anche alla più recente giurisprudenza. Ci si riferisce alla pronuncia in cui si legittima l'accertamento di fatti disciplinarmente rilevanti mediante filmati di telecamere installate in locali dove si erano verificati furti e ancora in ipotesi di mancata registrazione della vendita da parte dell'addetto alla cassa ed appropriazione delle somme incassate (cfr. Cass. n.17004/2024, con nota di S. GRIVET FETA' *Ancora sui controlli datoriali tramite agenzia investigativa: vietata ogni verifica collegata alla prestazione lavorativa e al suo (in)adempimento* in *www.rivistalabor.it, 29 agosto 2024*).

Resta invece privo di qualsivoglia approfondimento il mancato rispetto del tempo di conservazione delle video riprese di sette giorni, richiamato nell'accordo collettivo e totalmente disatteso dall'azienda. Il periodo massimo di conservazione dei dati non è definito da alcuna normativa.

Tuttavia, nel Regolamento generale sulla Protezione dei dati personali (Reg. UE n.2016/679 cd. GDPR) il principio di limitazione del trattamento indica che i dati personali possano essere trattati solo per il tempo indispensabile alle finalità decise dal datore di lavoro Titolare del trattamento (art.5 GDPR).

Inoltre, la norma precisa che tale tempo di conservazione massimo (o i criteri per la sua definizione) debba essere oggetto di informativa (art. 13 GDPR).

Qualora questi profili fossero stati approfonditi, avrebbero potuto comportare non certo l'installazione "non a norma" del sistema di videosorveglianza, bensì l'inutilizzabilità – per il datore di lavoro – delle videoriprese ai fini disciplinari per l'illegittimità del trattamento dei dati personali derivante dalla violazione della normativa in materia di protezione dei dati personali (cfr. artt.5 e 13 GDPR e art.2 decies d. lgs. 30 giugno 2003, n. 196 e s.m.i.).

Quanto al secondo motivo di gravame il ricorrente censura il fatto che l'estrazione delle videoriprese da parte dell'azienda non era stata rispettosa delle buone pratiche di *digital forensics* previste dalla legge n.48/2008.

La Corte considera inammissibile tale motivo di ricorso, nella parte in cui si deduce genericamente, e senza il rispetto della specificità, la violazione della legge n.48/2008 che riguarda i crimini informatici e contiene previsioni operanti nell'ambito dei procedimenti penali e non civili.

La contestazione del ricorrente attiene alla violazione dei paradigmi definiti a seguito della legge di ratifica della Convenzione di Budapest 23 novembre 2001 del Consiglio d'Europa volti all'acquisizione della prova digitale.

Si tratta dei principi che impongono di garantire l'assenza di alterazioni/danneggiamenti del dispositivo originale; l'autenticazione del reperto e dell'immagine acquisita; la garanzia della ripetibilità dell'accertamento; l'analisi senza modifica dei dati originari; la massima imparzialità nell'agire tecnico (cfr. E. Sanguedolce – C. Maioli, *I "nuovi" mezzi di ricerca del-*

la prova fra informatica forense e L. 48/2008 pubblicato in d. 07 maggio 2012 in www.altalex.com).

Gli ermellini osservano che le disposizioni richiamate della legge n.48/2008 attengono al processo penale. E che nel processo civile l'efficacia probatoria delle riproduzioni meccaniche (come i file delle videoriprese) è subordinata alla esclusiva volontà della parte contro cui vengono prodotte in giudizio ai sensi dell'art.2712 c.c.

In effetti, con la legge n.48/2008 di ratifica della Convenzione di Budapest, l'Italia ha aggiornato solo in ambito penale le proprie regole processuali di acquisizione delle prove digitali (cfr. F. Lazzini, *La Digital forensics nel processo penale: quadro normativo, giurisprudenza, diritto di difesa e aspetti di cyber security*, in www.ictsecuritymagazine.com).

Il codice di procedura penale è stato novellato in più disposizioni dedicate ai mezzi di ricerca della prova e alle indagini preliminari in presenza di prove digitali. Ed è stata codificata la necessità di adottare misure tecniche dirette a preservare l'integrità dei dati, assicurandone la conservazione e impedendone l'alterazione secondo le migliori tecniche di informatica giuridica (M. Torre, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48* in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 65-104, in www.ittig.cnr.it).

In ogni caso, gli ermellini ritengono irrilevante che i file del sistema di videosorveglianza, in quanto digitali, siano stati acquisiti senza i dettami imposti dalle buone prassi di *digital forensics*, che avrebbero imposto di acquisire una copia forense della memoria del sistema di videosorveglianza.

E osservano come la difesa dell'addetto alla biglietteria abbia formulato una censura di autenticità della prova digitale del tutto generica, priva di qualsivoglia specifico riferimento a circostanze concrete idonee ad attestare la non corrispondenza tra realtà fattuale e riprodotta.

Sicché, in assenza di un effettivo "disconoscimento" della videoripresa ai sensi dell'art.2712 c.c., il Giudice accerta la "piena prova" dei fatti riprodotti. Per evitare simile conseguenza processuale, il "disconoscimento" avrebbe dovuto essere chiaro, circostanziato ed esplicito ed avvenire nella prima udienza o nella prima risposta successiva alla rituale acquisizione delle suddette riproduzioni (Cass. n.8998/2001; Cass. n.2117/2011; Cass. n.3122/2015).

La Cassazione conferma quindi un consolidato orientamento che considera irrilevanti – nel processo civile – le prassi di *digital forensics*.

Ritiene il video del sistema di sorveglianza dedotto in giudizio come rappresentazione di atti, fatti o dati giuridicamente rilevanti ex art. 2712 c.c. con il risultato per cui «forma piena prova dei fatti e delle cose rappresentate se colui contro il quale viene prodotto non ne contesti la conformità ai fatti o alle cose medesime».

Una norma di chiusura, l'art.2712 c.c., a carattere generale, suscettibile di essere applicata anche a strumenti che non esistevano al momento dell'entrata in vigore del codice (S. Patti, *Della prova documentale*, in Commentario Scialoja-Branca, sub artt. 2699-2720, Bologna-Roma, Zanichelli, 1996, 126).

Poco importa per la Corte come sia stato raccolto e acquisito il file video. Irrilevante il fatto che la modalità più corretta e sicura di produzione della prova informatica sarebbe stata

quella della c.d. copia forense ("una copia fide facente dei dati in questione, ottenuta attraverso procedure e prassi tecnologiche specifiche atte a garantire la conservazione dell'integrità dei dati digitali originari (…) (inibendo) la manipolazione del dato" così S. Giorgi, *Prove digitali e processo tributario: orientamenti giurisprudenziali sull'utilizzabilità di messaggi istantanei e foto di schermate*, in *Rivista telematica di diritto tributario*).

Secondo la Corte, e la più recente giurisprudenza di merito, ciò che rileva nel processo civile è l'eventuale "disconoscimento" "*idoneo a (far) (…) perdere la qualità di prova (alle riproduzioni informatiche), degradandole a presunzioni semplici"* purché *"chiaro, circostanziato ed esplicito, dovendosi concretizzare nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta"* (Tribunale Cremona, 23 novembre 2023).

Un disconoscimento che tuttavia non può limitarsi a formule di stile poiché la parte che disconosce la "rappresentazione meccanica di fatti" è onerata dell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta (Tribunale Milano, Sez. VI, Sentenza, 21 aprile 2022, n. 3470).

La pronuncia in commento, seppure condivisibile, deve far riflettere in merito all'esigenza di assicurare, come operatori del diritto, la genuinità della prova "digitale", per sua stessa natura volatile e fragile (A. d'Arminio Monforte – M. Rocchi, *Le prove digitali nel processo civile*, 2021, Pacini Giuridica).

Qualora l'azienda avesse provveduto ad estrarre il video dal sistema di sorveglianza effettuando una copia forense dell'archivio digitale, non si sarebbe esposta. L'utilizzo delle tecniche *standard* per la clonazione del contenuto di un dispositivo, capaci di garantirne l'immodificabilità e consentire un controllo sulla corrispondenza tra quanto depositato e l'originale, avrebbe evitato agevoli contestazioni (A. Larussa – P. Pellegrinelli, *Le prove digitali nel processo*, Milano Giuffré 2023). Il progredire della pervasività della trasformazione digitale impone di riflettere sull'acquisizione delle prove digitali e ciò per evitare contestazioni riguardo potenziali manipolazioni, cancellazioni o alterazione dei dati dedotti in giudizio. Le garanzie di integrità, non manipolabilità e autenticità del dato sono e saranno sempre più di attualità, considerando gli sviluppi dei sistemi di intelligenza artificiale e dei dispositivi capaci di consentire manipolazioni di foto, audio, filmati.

Claudia Ogriseg, avvocato in Udine

Visualizza il documento: Cass., ordinanza 6 settembre 2024, n. 23985