Tutela del patrimonio aziendale

Videosorveglianza: limiti di legittimità dei controlli difensivi

Alessia La Mendola - Funzionario della Agenzia delle entrate direzione provinciale di Monza e Brianza

In tema di applicabilità dell'art. 4, Statuto dei lavoratori ad una fattispecie anteriore alle modifiche apportate dal D.Lgs. n. 151/2015, attuativo di una delle deleghe contenute nel c.d. Jobs Act, con particolare riferimento ai limiti di legittimità dei c.d. controlli difensivi, una particolare rilevanza assume la sentenza della Corte di cassazione n. 22662 dell'8 novembre 2016, nella quale i giudici di legittimità hanno affermato che "*in tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, legge n. 300/1970, espressamente richiamato dall'art. 114, D.Lgs. n. 196/2003, per l'installazione di impianti e apparecchiature di controllo, richiesti da esigenze organizzative e produttive, ovvero dalla sicurezza del lavoro, dai quali derivi la possibilità di verifica a distanza dell'attività dei lavoratori, trovano applicazione ai controlli, c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso. Ne consegue che esula dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale*".

Prima di riassumere la vicenda sottesa alla menzionata pronuncia, al fine di un esauriente trattazione dell'argomento in esame, e richiamare le motivazioni dei giudici di legittimità nella sentenza n. 22662/2016, occorre analizzare la normativa relativa ai controlli a distanza sui lavoratori alla luce delle modifiche apportate dal D.Lgs. n. 151/2015, attuativo di una delle deleghe contenute nel c.d. Jobs Act, ed i precedenti orientamenti giurisprudenziali in materia.

I controlli a distanza sui lavoratori prima e dopo i Decreti attuativi del Jobs Act

I controlli a distanza sui lavoratori sono disciplinati dall'art. 4, legge n. 300/1970, così come modificato dall'art. 23, D.Lgs. n. 151/2015.

Si definiscono controlli a distanza quei poteri di vigilanza, esercitati dal datore di lavoro, in qualità di capo dell'impresa *ex* art. 2086 c.c., mediante impianti e strumenti da posizioni geograficamente diverse ed in periodi successivi rispetto al tempo ed al luogo in cui viene eseguita la prestazione lavorativa (1).

La *ratio* ispiratrice delle modifiche apportate dal legislatore è indubbiamente riconducibile alle moderne tecnologie telematiche, che hanno reso ineluttabile l'aggiornamento di norme emanate quando telefoni cellulari e *smartphone*, personal *computer* e *tablet*, *internet*, posta elettronica erano per lo più ancora in fase di ideazione (2).

Pertanto il nuovo art. 4, legge n. 300/1970 mira a contemperare la fisiologica evoluzione degli strumenti adoperati nel sistema di organizzazione del lavoro con incontrovertibili limiti da apporre ai poteri direttivi del datore di lavoro nel caso in

(1) Goffredo M.T. e Meleca V., *Job act* e nuovi controlli a distanza in *Diritto e pratica del lavoro* 31/2016.

(2) Cfr Meleca V., *Il Grande fratello in azienda* in *Diritto e pratica del lavoro* 1993 pag. 2927; e *Il Grande fratello in azienda - tra privacy e controlli a distanza*, *Isper*, 2002.

cui quest'ultimi intacchino eccessivamente la sfera dei diritti inviolabili dei lavoratori (3).
Ergo, in base al riformato art. 4, Statuto dei lavoratori, gli impianti audiovisivi e gli altri strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (4).
Tali tecnologie, quindi, possono essere installate previo accordo collettivo stipulato dalle rappresentanze sindacali unitarie o dalle rappresentanze sindacali aziendali, ed, in alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione, ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale (5).
Inoltre, aggiunge la disposizione che, in mancanza di tale accordo, gli impianti e gli strumenti *de quibus* possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.
Infine, il legislatore chiarisce che la nuova disciplina non si applica agli strumenti utilizzati dal lavoratore per eseguire la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze, ed, in ogni caso, il datore di lavoro è obbligato a dare al lavoratore adeguate informazioni sulle modalità d'uso degli strumenti e di effettuazione dei controlli nel rispetto di quanto disposto dal Decreto legislativo 30 giugno 2003, n. 196.
Le novità del nuovo art. 4, Statuto dei lavoratori riguardano, dunque, i seguenti aspetti.
In primis viene previsto un doppio regime: uno per gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori; l'altro, invece, rivolto agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
In particolare, in riferimento agli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, rispetto al precedente testo dell'art. 4 Stat. lav., alle esigenze organizzative e produttive ed alla sicurezza del lavoro si aggiunge la tutela del patrimonio aziendale, quale causa di legittimazione per l'installazione degli apparecchi *de quibus.*
Inoltre, sempre in riferimento a tali impianti, rispetto alla precedente versione della norma si prevede che le imprese con più unità produttive ubicate in diverse Province della stessa Regione o in più Regioni, anziché dover sottoscrivere accordi con le Rappresentanze sindacali unitarie od aziendali per ogni singola unità produttiva, hanno con la nuova formulazione dell'art. 4, Stat. lav. la possibilità di sottoscrivere accordi con le associazioni sindacali territoriali o nazionali comparativamente più rappresentative sul piano nazionale.
Invece, in riferimento agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa ed agli strumenti di registrazione delle presenze e degli accessi, il datore di lavoro non è più tenuto né ad accordi con le rappresentanze sindacali, né a richiedere autorizzazioni da parte della Direzione territoriale del lavoro o del Ministero del lavoro.
In secundis l'altra novità del Jobs Act sull'art. 4, Stat. lav. riguarda il terzo comma, il quale prevede espressamente, nel rispetto di quanto disposto dal D.Lgs. n. 196/2003 in materia di tutela della *privacy*, l'obbligo di fornire al lavoratore adeguate informazioni circa le modalità d'uso degli strumenti di controllo, le tipologie di verifiche da effettuare, i nominativi dei soggetti preposti ai controlli, la periodicità o l'occasionalità degli accertamenti, il tipo di programmi informatici utilizzati.
Questo tipo di obblighi informativi riguarda ad esempio i telefoni aziendali (fissi e cellulari), ovvero la navigazione in *internet* o la posta elettronica, specificando quali comportamenti sono tollerati o vietati all'interno dell'impresa (6).

(3) Cfr Del Punta R., *La nuova disciplina del controllo a distanza sul lavoro (art. 23, D.Lgs. n. 151/2015)*, in *RidI*, 1/2016.
(4) Cfr Carinci M.T. *Il controllo a distanza dell'attività dei lavoratori dopo il Job Act (art. 23, D.Lgs. n. 151/2015): spunti per un dibattito* in *Labour &law iussues,* Volume n. 2/2016; Goffredo M.T. e Meleca V., *Job act e nuovi controlli a distanza* in *Diritto e pratica del lavoro* 31/2016.
(5) Cfr Alvino I., *L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica*, in *Dri*, 4/2014, pag. 999.
(6) Cfr Iaquinta F., Ingrao A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Dri*, 4/2014, pag. 1027.

In particolare si devono precisare quali informazioni sono oggetto di temporanea memorizzazione; per quanto tempo i dati verranno conservati e potranno, quindi, essere controllati dal datore di lavoro; chi è il responsabile del trattamento dei dati acquisiti, al quale il dipendente può rivolgersi per tutte le questioni relative all'impiego, alla conservazione o all'utilizzo dei propri dati personali; le conseguenze di carattere disciplinare che possono derivare dal non corretto uso degli impianti e degli strumenti in oggetto (7).

A tal proposito, sulle riforme attuate dal D.Lgs. n. 151/2015 all'art. 4, legge n. 300/1970 assume particolare rilievo il Provvedimento n. 303 del 13 luglio 2016 del Garante per la protezione dei dati personali.

In particolare l'Autority ha operato una distinzione tra gli "strumenti di lavoro", rispetto ai quali non sono necessari accordi con le rappresentanze dei lavoratori né, in subordine, le autorizzazioni amministrative; e altri strumenti che non possono essere ascritti alla categoria degli strumenti di lavoro, *sic et simpliciter*, e che, pertanto, rientrano nella categoria degli strumenti di controllo a distanza dell'attività dei lavoratori.

Pertanto, a parere del Garante, appartengono alla prima categoria il servizio di posta elettronica (con attribuzione di un account personale) e internet, così come i vari software finalizzati alla tutela del patrimonio della rete telematica dell'impresa (si pensi ai sistemi di *logging* ed ai programmi antivirus).

Rientrano, invece, nella seconda categoria gli strumenti che consentono di svolgere un'attività di controllo in *background*, ed in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore, attraverso il ricorso ad operazioni di filtraggio, blocco, controllo e tracciatura costanti. Per tali strumenti si rientra nella fattispecie normata dall'art. 4, legge n. 300/1970, con la conseguente applicazione delle regole ivi previste (8).

Dunque, sebbene la recente riforma del lavoro, intervenendo sull'art. 4, Stat. lav., ha allargato le maglie sull'utilizzo di strumenti che possono consentire anche un monitoraggio dei dipendenti, il controllo a distanza sui lavoratori deve tenere conto di alcuni vincoli, imposti dal Garante della *privacy*, che ha provveduto a mettere gli opportuni paletti al fine di consentire l'installazione di tali apparecchi solo come *extrema ratio* qualora l'utilizzo di tali impianti fosse sfornito dei necessari accordi sindacali o dell'autorizzazione della Direzione territoriale del lavoro (9).

Gli orientamenti giurisprudenziali

Un importante precedente giurisprudenziale della Corte di cassazione, nella tematica, riguardante la sentenza in commento, si rinviene nella sentenza della Corte di cassazione n. 15892/2007, che ha sancito l'applicabilità nel caso in esame dell'obbligo di accordo sindacale a un impianto automatico di controllo accessi a un parcheggio aziendale, e nella sentenza n. 4375/2012, con la quale la Corte di cassazione ha sancito l'applicabilità dell'art. 4, comma 2, Stat. lav. ai sistemi di *content filtering* (10).

Secondo la Corte di cassazione, infatti: "*i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento (se non altro, nel nostro caso, sotto il profilo del rispetto delle direttive aziendali)", e ciò "è evidente laddove nella lettera di licenziamento i fatti accertati mediante il programma Super Scout sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza sub specie di aver utilizzato tempo lavorativo per scopi personali (e non si motiva invece su una particolare pericolosità dell'attività di collegamento in rete rispetto all'esigenza di protezione del patrimonio aziendale)*".

Nel vasto panorama giurisprudenziale pronunciatosi *ratione materiae* altro importante contributo è stato offerto dalla sentenza della Corte di cassazione n. 2722/2012, in base alla quale si può adottare un'interpretazione meno rigida dell'art. 4, comma 2, Stat. lav. nell'ipotesi di controlli

(7) Cfr Dui P. *I controlli a distanza: la negazione del tertium genus* in *Lav. nella giur.* 2010, pag. 90.

(8) Modesti G. *Controllo a distanza dei lavoratori: il parere del Garante* in *Fisco e Tasse* 14 ottobre 2016.

(9) Cherchi A., *Controlli a distanza: limiti del garante* in *Il Sole - 24 ore*, 16 settembre 2016.

(10) Faggioli G. *Job act più chiarezza nei controlli a distanza con la bozza di riforma* in *Corriere comunicazione* 15 giugno 2015.

reattivi avverso un'aggressione di un bene tutelato di titolarità dell'azienda.
Infatti in presenza di tale condizione, secondo i giudici di legittimità, "*il datore di lavoro aveva compiuto un accertamento ex post quando erano emersi elementi di fatto tali da raccomandare l'avvio di una indagine retrospettiva" che "il controllo difensivo non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro ma era destinato ad accertare un comportamento che metteva in pericolo l'immagine del datore di lavoro" e quindi che "tale situazione è già esclusa dal campo di applicazione dell'art. 4, comma II, Statuto dei lavoratori*".
Infine si rammenti la recentissima sentenza della Corte di cassazione n. 22313 del 3 novembre 2016, che contempla una fattispecie del tutto analoga alla vicenda giuridica *de qua,* ed ove i giudici di legittimità hanno statuito che "*il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 c.c.), tra cui i pc aziendali. Nell'esercizio di tale prerogativa, occorre tuttavia rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali dettata dal D.Lgs. n. 196/2003, i principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11, comma 1, Codice della privacy. Ciò, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile".*
Con tale sentenza, quasi contemporanea alla sentenza oggetto del contributo, la Suprema Corte ha cassato una sentenza della Corte d'Appello, che aveva dichiarato l'illegittimità del licenziamento intimato a un dipendente, a seguito di contestazione disciplinare con la quale si riferiva che nel corso di un'ispezione volta alla verifica del rispetto delle disposizioni interne in materia di uso e sicurezza del materiale informatico assegnato ai dipendenti, questi, alla richiesta di chiarimenti in ordine ad alcuni file con estensione video contenuti nel disco O, aveva cancellato l'intero contenuto del disco, rendendo impossibile dare seguito all'attività ispettiva.
All'esito di un successivo esame dell'archivio informatico, dove il materiale era custodito, era emersa la presenza di materiale con contenuto pornografico.
Alla luce di tutto ciò, la contestazione riguardava *in primis* l'aver ostacolato l'attività ispettiva del servizio revisione; *in secundis* la violazione dell'obbligo di tenere una condotta informata ai principi di disciplina, dignità e moralità; *in tertiis* il fatto di non dedicare il tempo lavorativo esclusivamente all'attività aziendale; *in quartis* la violazione del codice di comportamento che prescrive che i dipendenti della cassa sono tenuti ad utilizzare le apparecchiature esclusivamente per finalità di ufficio, nonché l'aver esposto il datore di lavoro ai rischi conseguenti l'acquisizione nel proprio sistema informatico di file che avrebbero potuto comportare sanzioni ai sensi del D.Lgs. n. 231/2001 (11).
Va rilevato che anche questo caso è anteriore al D.Lgs. n. 151/2015.
In proposito, la Cassazione ha giustamente evidenziato che la questione giuridica sottesa non attiene alla materia dei c.d. controlli a distanza, né all'utilizzo dei dati desunti dal computer aziendale, ma al potere di controllo del datore di lavoro sull'utilizzo dello strumento presente sul luogo di lavoro e in uso al lavoratore per lo svolgimento della prestazione.
In merito, la Suprema Corte ha richiamato l'Autorità del Garante alla privacy, che è più volte intervenuta per cercare di risolvere le problematiche sorte in relazione alla crescente necessità di evoluzione tecnologica delle aziende e al connesso utilizzo degli strumenti informatici da parte dei lavoratori, statuendo il principio in base al quale una società non può controllare il contenuto del pc di un dipendente senza averlo prima informato sui limiti di utilizzo del bene aziendale, e sulla possibilità che possano essere avviate penetranti operazioni di analisi e verifica sulle informazioni contenute nel pc stesso.

(11) Rocchetti P., *I limiti al potere di controllo del datore di lavoro sulle condotte del lavoratore. Commento alle sentenze n. 22662/2016 e 22213/2016 della Cassazione* in *Questione Giustizia* 30 novembre 2016.

La decisione della Suprema Corte n. 22662/2016

Nella vicenda giuridica, oggetto della sentenza n. 22662/2016 in commento, un'azienda ricorreva avverso la sentenza della Corte d'Appello, che aveva dichiarato illegittimo il licenziamento per giusta causa intimato a una lavoratrice, alla quale era stato contestato di avere sottratto una busta contenente denaro dalla cassaforte aziendale.
In particolare la dipendente aveva sfilato tale busta dalla fessura con un tagliacarte e l'addebito di tale condotta era stata ricavata da un filmato prodotto da una telecamera, preposta al controllo della predetta cassaforte.
In particolare, la Corte territoriale fondava la decisione sul rilievo che l'installazione dell'impianto audiovisivo se da un lato era astrattamente legittima *ex* art. 4, comma 2, legge n. 300/1970 in quanto giustificata dalle esigenze di tutela dei beni aziendali, nonché di sicurezza dei lavoratori operanti in *reception* vicino a un obiettivo sensibile, quale la cassaforte; dall'altro lato, tuttavia, avrebbe richiesto in concreto il previo accordo con le rappresentanze sindacali aziendali o con la commissione interna o, in mancanza di accordo, l'autorizzazione dell'Ispettorato del lavoro.
Infatti tale apparecchio audiovisivo, sebbene non direttamente finalizzato al controllo a distanza della prestazione lavorativa degli addetti alla *reception*, consentiva, comunque, di vigilare sugli spostamenti dei dipendenti nell'ambiente di lavoro con la conseguenza che, in mancanza delle prescritte autorizzazioni, il filmato era da ritenere inutilizzabile ed era da espungere dal materiale probatorio acquisibile.
Pertanto, a parere dei giudici di merito, pur in presenza della prova dell'ammanco di denaro, veniva a mancare la prova dell'addebitabilità del fatto contestato, ed il licenziamento era da considerarsi illegittimo.
Avverso la sentenza della Corte d'Appello la società propone ricorso per cassazione sulla base di due motivi.
In primis la ricorrente deduce la violazione dell'art. 4, legge n. 300/1970.
Infatti, secondo parte attrice, tale disposizione non si riferisce a qualsiasi attività svolta dai lavoratori all'interno dell'azienda.
Al contrario tale controllo difensivo richiede il vaglio della procedura contrattuale solo se da esso derivi la possibilità di un controllo a distanza dell'attività dei lavoratori, che verta sull'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non sulla tutela dei beni estranei a tale rapporto.
Pertanto, a parere della società, il controllo è legittimo, e non richiede alcuna procedura preventiva, qualora non riguardi in alcun modo l'attività lavorativa, ma sia unicamente diretto ad accertare eventuali condotte illecite dei lavoratori o di terzi, e risulti indispensabile per la tutela del patrimonio aziendale.
In secundis l'azienda datrice di lavoro contesta la violazione degli articoli 11 e 160, D.Lgs. n. 196/2003 in quanto le prove acquisite mediante l'utilizzo di apparecchiature audio visive, a differenza da quanto asserito dai giudici d'appello, sono sempre utilizzabili nell'ipotesi di addebito mosso al dipendente che implichi un illecito, riconducibile nel caso *sub specie* ad un attentato al patrimonio del datore di lavoro.
La Suprema Corte nella sentenza, oggetto del contributo, accoglie i motivi del ricorso per le ragioni di cui *infra.*
A parere degli Ermellini, i controlli difensivi di cui all'art. 4, comma 2, Stat. lav., nel testo vigente all'epoca dei fatti, richiedono il previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna, solo nel caso in cui da essi derivi anche la possibilità di vigilare a distanza l'esatto adempimento delle prestazioni lavorative.
Al contrario tali controlli non richiedono dette garanzie procedurali laddove si limitino ad accertare comportamenti illeciti dei lavoratori lesivi del patrimonio e dell'immagine aziendale.
Secondo la Corte di cassazione nella decisione n. 22662/2016, dunque, nel caso in disamina la condotta della lavoratrice, oggetto della ripresa video, è identica a qualunque comportamento illecito posto in essere da un qualsiasi soggetto estraneo all'organizzazione del lavoro.
Pertanto, il controllo difensivo attuato non attiene all'adempimento delle obbligazioni del rapporto di lavoro.
Infatti, al contrario, i giudici di legittimità statuiscono che tale tipologia di controllo era finalizzato a prevenire un pericolo per la sicurezza dei lavoratori e per il patrimonio aziendale, risultando incontrovertibile il diritto del datore di lavoro a tutelare la propria azienda mediante gli stru-

menti connessi all'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.
Dunque, a parere della Suprema Corte nella sentenza n. 22662/2016, la tutela del diritto alla riservatezza ed alla dignità del lavoratore non consente di escludere dal campo di applicazione dell'art. 4, Stat. lav. i controlli diretti ad accertare comportamenti illeciti di dipendenti o di terzi *a fortiori* quando, come nella vicenda giuridica *de qua,* la telecamera, per la posizione e il campo visivo coperto, era stata installata per sorvegliare la cassaforte anche a garanzia della sicurezza degli altri lavoratori operanti alla *reception*, con postazione vicina ad un possibile obiettivo di malintenzionati, e comunque esposti ai rischi derivanti dall'essere a contatto con il pubblico.

Conclusioni

La decisione della Suprema Corte rileva l'estrema attualità della questione relativa al controllo a distanza dei lavoratori nell'ipotesi di rischi per la sicurezza dei lavoratori e per l'integrità del patrimonio aziendale, introducendo, quale *quid pluris,* il principio in base al quale è legittimo l'utilizzo delle innovazioni tecnologiche, che *incidenter tantum* possano vigilare sugli spostamenti dei lavoratori, nel rispetto di dettagliate causali relative a esigenze organizzative e produttive, sicurezza sul lavoro, e tutela del patrimonio aziendale.
La base normativa della sentenza in commento poggia senza dubbio sulla precedente disciplina dell'art. 4, Statuto dei lavoratori, il quale sanciva un divieto assoluto del così detto controllo intenzionale, finalizzato alla mera vigilanza dell'attività lavorativa, temperando il rigore di tale divieto in presenza dei così detti "controlli difensivi", finalizzati a prevenire un comportamento illecito del lavoratore sulla base di indizi o sospetti di colpevolezza.
Infatti, come si evince dal P.Q.M. della Suprema Corte, se è vero che il nuovo art. 4, Statuto dei lavoratori, alla luce delle novità normative di cui al D.Lgs. n. 151/2015, giustifica l'uso degli impianti audio visivi *de quibus* alla *condicio sine qua non* che i datori di lavoro si dotino di *policy* interne, che disciplinino in maniera puntuale e trasparente l'utilizzo di tali sistemi informatici nel rispetto delle prescrizioni contenute nel Codice in materia di protezione dei dati personali; è altrettanto inequivocabile un diritto del datore di lavoro ad esigere dal dipendente la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale ai sensi dell'art. 2104 c.c.
Pertanto, il diritto del lavoratore alla libertà ed alla riservatezza, incontrovertibilmente sancito dall'art. 8 della Convenzione per la protezione dei diritti dell'uomo, ha un rapporto di necessaria complementarietà, e non di contrarietà, con l'articolo 41, Costituzione, il quale non potrebbe tutelare la libera iniziativa economica del datore di lavoro qualora nel mercato del lavoro non si garantisse la corretta applicazione delle sottostanti norme di cui agli articoli 2086 e 2094, Codice civile, esigendo l'obbligo di sicurezza, che incombe in capo all'imprenditore, una doverosa collaborazione diligente da parte del lavoratore ai fini di un'efficiente e produttiva organizzazione aziendale.

La sentenza

Corte di cassazione, 8 novembre 2016, n. 22662
Furto - Impianto di videosorveglianza - Estraneità rispetto alla prestazione lavorativa - Controlli difensivi - Legittimità - Ricorso - Accolto

Svolgimento del processo

1. Con sentenza depositata il 30 gennaio 2014 la Corte d'Appello di Torino, in riforma della decisione del giudice di primo grado, ha dichiarato illegittimo il licenziamento per giusta causa intimato a (...) dipendente della società con mansioni di addetta alla segreteria e all'accoglienza clienti, da (...) società svolgente attività fisioterapica poliambulatoriale.
2. Alla lavoratrice era stato contestato di aver sottratto, tra il 24 e il 25 gennaio 2012, una busta contenente denaro dalla cassaforte aziendale, sfilandola dalla fessura con un tagliacarte. La condotta era ricavabile da un filmato prodotto da una telecamera preposta al controllo della predetta cassaforte.
3. La Corte territoriale fondava la decisione sul rilievo che l'installazione dell'impianto audiovisivo, pur astrattamente legittima *ex* art. 4, c. II, legge 300/1970, in quanto sorretta dalle esigenze dedotte dalla società (tutela dei beni aziendali, nonché tutela della sicurezza dei lavoratori operanti in reception vicino a un possibile obietti-

vo di malintenzionati), avrebbe richiesto il previo accordo con le rappresentanze sindacali aziendali o con la commissione interna o, in mancanza di accordo, l'autorizzazione dell'Ispettorato del lavoro. E ciò in quanto, ancorché non diretta al controllo a distanza della prestazione lavorativa delle addette alla reception, consentiva il controllo degli spostamenti dei dipendenti nell'ambiente di lavoro. In mancanza delle prescritte autorizzazioni il filmato era da ritenere inutilizzabile e, espungendo lo stesso dal materiale probatorio, pur in presenza della prova dell'ammanco di denaro, veniva a mancare la prova dell'addebitabilità del fatto contestato.
3. Avverso la sentenza propone ricorso per cassazione la (...) sulla base di due motivi, illustrati con memoria. Resiste la (...) con controricorso.

Motivi della decisione

1. Con il primo motivo la ricorrente deduce violazione e falsa applicazione di norme di diritto *ex* art. 360, n. 3 c.p.c. e segnatamente dell'art. 4, legge n. 300/1970. Osserva che la Corte territoriale, laddove ha ritenuto che l'art. 4, c. 1, legge n. 300/1970 faccia riferimento all'attività dei lavoratori, intesa come qualsivoglia attività svolta dai lavoratori all'interno dell'azienda senza distinzioni, ha falsamente applicato la norma, dando un'interpretazione assolutamente contrastante con la giurisprudenza di legittimità. Secondo tale giurisprudenza il controllo difensivo richiede il vaglio della procedura contrattuale solo se da esso derivi la possibilità di controllo a distanza dell'attività dei lavoratori, cioè l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela dei beni estranei al rapporto stesso.
Con la conseguenza che il controllo è legittimo e non rientrante nella procedura richiamata qualora non riguardi in alcun modo l'attività lavorativa, ma sia unicamente diretto ad accertare eventuali condotte illecite dei lavoratori o di terzi e risulti indispensabile per la tutela del patrimonio aziendale. Osserva che la Corte territoriale aveva omesso totalmente di esaminare se la ripresa degli spostamenti dei dipendenti avesse leso la dignità e la riservatezza degli stessi.
2. Con il secondo motivo la ricorrente deduce violazione e falsa applicazione di norme di diritto *ex* art. 360, n. 3 e segnatamente dell'art. 4, legge n. 300/1970 e degli artt. 11 e 160, D.Lgs. 196/2003. Rileva che, anche a ritenere fondata la tesi sostenuta in sentenza in punto di applicazione del citato art. 4, in ogni caso la prova acquisita mediante l'utilizzo di apparecchiature vietate è utilizzabile, assumendo rilievo il tipo di addebito mosso al dipendente. Laddove l'addebito riguardi un illecito del dipendente ovvero un attentato al patrimonio del datore di lavoro, le prove devono ritenersi sempre utilizzabili.
3. I motivi possono essere trattati congiuntamente in ragione dell'intima connessione. La questione sottoposta all'attenzione di questa Corte concerne i limiti di legittimità dei c.d. controlli difensivi, controlli finalizzati non già a verificare l'esatto adempimento delle obbligazioni direttamente scaturenti dal rapporto di lavoro, ma a tutelare beni del patrimonio aziendale e ad impedire la perpetrazione di comportamenti illeciti. I suddetti controlli, *ex* art. 4, comma 2, Statuto dei lavoratori, nel testo vigente all'epoca dei fatti, richiedono il "previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna" solo nel caso in cui da essi "derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" (in tal senso Cass., sez. L, n. 2722 del 23 febbraio 2012, Rv. 621115: "In tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, legge n. 300/1970, espressamente richiamato dall'art. 114, D.Lgs. n. 196/2003, per l'installazione di impianti e apparecchiature di controllo richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, dai quali derivi la possibilità di verifica a distanza dell'attività dei lavoratori, trovano applicazione ai controlli, c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso. Ne consegue che esula dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale. (In applicazione del suddetto principio, è stato ritenuto legittimo il controllo effettuato da un istituto bancario sulla posta elettronica aziendale del dipendente accusato di aver divulgato notizie riservate concernenti un cliente, e di aver posto in essere, grazie a tali informazioni, operazioni finanziarie da cui aveva tratto vantaggi propri)".
4. Nel caso in disamina la condotta della lavoratrice oggetto della ripresa video non solo non atteneva alla prestazione lavorativa ma non differiva in alcun modo da quella illecita posta in essere da un qualsiasi soggetto estraneo all'organizzazione del lavoro. Il c.d. controllo difensivo, pertanto, non atteneva all'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa sicurezza dei lavoratori, oltre al patrimonio aziendale, determinando la diretta implicazione del diritto del datore di lavoro di tutelare la propria azienda mediante gli strumenti connessi all'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.
5. Per altro verso, va rilevato che la giurisprudenza di questa Corte ha avuto modo di chiarire che l'art. 4 "fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore ... sul presupposto - espressamente precisato nella Relazione ministeriale - che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada

mantenuta in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro" (Cass. 17 luglio 2007, n. 15982; conforme Cass. 23 febbraio 2012, n. 621115). La tutela del diritto alla riservatezza non consente di escludere che rientrino nella fattispecie di cui al citato art. 4 i controlli diretti ad accertare comportamenti illeciti dei lavoratori nel caso in cui la sorveglianza riguardi l'espletamento dell'attività lavorativa e venga attuata mediante strumenti potenzialmente lesivi della sfera personale, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro. E' stato precisato che in tal caso si è di fronte a "un controllo cd. preterintenzionale che rientra nella previsione del divieto flessibile di cui all'art. 4, comma 2" (Cass. 23 febbraio 2010, n. 4375), rimanendo in tal modo superata una precedente impostazione che riteneva in ogni caso legittimi i c.d. controlli difensivi, a prescindere dal loro grado di invasività (Cass. 3 aprile 2002, n. 4746).

6. Il ragionamento della Corte territoriale non fa corretta applicazione del dato normativo, nei termini ritenuti dalla richiamata giurisprudenza, alla quale questa Corte intende dare continuità. I giudici di merito, infatti, pur dando atto che la telecamera, per la posizione e il campo visivo coperto, era stata installata per sorvegliare la cassaforte "anche a garanzia della sicurezza dei lavoratori operanti alla reception, che si trovano vicino ad un possibile obiettivo di malintenzionati (la cassaforte, appunto) e comunque esposti ai rischi derivanti dall'essere il centro necessariamente aperto al pubblico", e pur rilevando che la medesima non consentiva un reale ed effettivo controllo a distanza della prestazione lavorativa, ha ritenuto l'installazione dell'impianto audiovisivo soggetta alla procedura di cui al comma secondo del citato art. 4 per il solo fatto che mediante lo stesso fosse consentito controllare gli spostamenti dei lavoratori nell'ambiente di lavoro, al di fuori dell'adempimento della prestazione. Da ciò ha tratto l'inutilizzabilità del filmato a fini disciplinari, senza neppure indicare elementi da cui trarre che le riprese abbiano potuto ledere la riservatezza dei lavoratori.

7. In base alle svolte argomentazioni il ricorso va accolto, con rinvio alla Corte di merito che provvederà anche alla liquidazione delle spese del presente giudizio di legittimità e si atterrà al seguente principio di diritto: "non è soggetta alla disciplina dell'art. 4, c. 2, Statuto dei lavoratori l'installazione di impianti e apparecchiature di controllo poste a tutela del patrimonio aziendale dalle quali non derivi anche la possibilità di controllo a distanza dell'attività lavorativa, né risulti in alcun modo compromessa la dignità e la riservatezza dei lavoratori".

P.Q.M.

Accoglie il ricorso, cassa la sentenza impugnata e rinvia, anche per le spese del giudizio di legittimità, alla Corte d'Appello di Torino in diversa composizione.