Uso di materiale informatico

Controllo del pc assegnato al lavoratore: licenziamento

Salvatore Servidio - Esperto tributario del processo del lavoro

La vicenda

Nell'articolata vicenda di fatto, la sentenza 3 novembre 2016, n. 22313 della Corte di cassazione rileva 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, un dipendente, alla richiesta di chiarimenti in ordine ad alcuni files con estensione video contenuti nel disco O, cancellava l'intero contenuto del disco, rendendo impossibile dare seguito all'attività ispettiva. All'esito di un successivo esame dell'archivio informatico, era emersa la presenza di materiale con contenuto pornografico.

Alla luce di tutto ciò il datore di lavoro intimava il licenziamento contestando al lavoratore:

- di aver ostacolato l'attività ispettiva del servizio revisione;
- di avere violato l'obbligo di tenere una condotta informata ai principi di disciplina, dignità e moralità sia in sede di effettuazione delle attività di revisione, sia acquisendo e conservando nel computer aziendale materiale pornografico;
- di avere violato l'obbligo di dedicare il suo tempo lavorativo all'attività aziendale;
- di avere violato il codice di comportamento che prescrive che i dipendenti sono tenuti ad utilizzare le apparecchiature esclusivamente per finalità di ufficio;
- di aver esposto la cassa ai rischi conseguenti l'acquisizione nel proprio sistema informatico di files "pericolosi".

Nel conseguente giudizio di opposizione la Corte d'Appello, confermando la sentenza di primo grado, riteneva che il licenziamento fosse illegittimo per insussistenza del fatto contestato - accordandogli la tutela di cui all'art. 18, comma 4, legge 20 maggio 1970, n. 300, come novellato della legge 28 giugno 2012, n. 92, c.d. legge Fornero -, considerato che il datore di lavoro non aveva dimostrato l'esistenza di documenti di pertinenza aziendale all'interno della parte del disco fisso del pc che era stata cancellata dal lavoratore.

Inoltre, il comportamento doveva ritenersi senz'altro scusabile in considerazione del fatto che gli ispettori avevano travalicato i propri poteri, imponendo al lavoratore l'immediata visione dei files, con richiesta abusiva perché sproporzionata e tale da lederne la privacy.

Nel conseguente ricorso per Cassazione, il datore di lavoro per quanto qui di interesse, critica la motivazione della Corte d'Appello, laddove ha ritenuto che gli ispettori avrebbero ecceduto dai propri poteri, potendo rinviare ad un secondo momento la visione del files sospetti, conservati nel server, anziché procedere in presenza dei colleghi.

Tale affermazione viene censurata sotto un primo profilo per violazione dell'art. 6 Cedu e artt. 115 e 116 c.p.c. oltre che per omesso esame di un fatto decisivo per il giudizio, in quanto la ricostruzione dei fatti posti dalla Corte d'Appello alla base della propria decisione non corrisponderebbe ai fatti dedotti e provati, poiché gli ispettori non chiesero al ricorrente di aprire i files, ma si limitarono a chiedere informazioni al riguardo e, dopo che il dipendente ne aveva cancellati alcuni, lo avevano invitato a non cancellarne ulteriori perché ciò avrebbe costituito un ostacolo all'attività ispettiva. Inoltre, l'attività di backup del server non aveva garantito l'integrale conservazione del contenuto ed era stato possibile recuperare solo i files risalenti sino a due giorni prima dell'ispezione. Aggiunge che al fatto erano presenti anche altri soggetti. Né i giudici di merito avrebbero ammesso la richiesta, su tali circostanze, di prova diretta e controprova.

Con un secondo profilo censorio, la ricorrente denuncia le argomentazioni della Corte territoriale per violazione del Codice in materia di protezione dei dati personali di cui al D.Lgs. 30 giugno 2003, n. 196 e dell'art. 2104 c.c., concernente la diligenza del prestatore di lavoro, in quanto chi è chiamato a verificare il rispetto delle norme in materia di sicurezza informatica può apprendere il contenuto dei files che si trovano nello strumento informatico affidato dall'azienda al lavoratore, sicché la condotta di chi impedisca tale verifica deve essere qualificata come illegittima.

Trattamento dei dati personali

Per inerenza all'argomento trattato, si premette che, poiché che ogni libertà civile trova il proprio limite nell'altrui libertà e nell'interesse pubblico idoneo a fondare l'eventuale sacrificio dell'interesse del singolo, deve anzitutto osservarsi che la tutela del diritto alla riservatezza va contemperata in particolare con il diritto di ed alla informazione, nonché con i diritti di cronaca, di critica, di satira e di caricatura, questi ultimi trovanti a loro volta limite nel diritto all'identità personale o morale del soggetto cui l'informazione si riferisce.
Il diritto alla riservatezza, che tutela il soggetto dalla curiosità pubblica (in ciò distinguendosi dal diritto al segreto, il quale protegge dalla curiosità privata) essendo volto a tutelare l'esigenza che quand'anche rispondenti a verità i fatti della vita privata non vengano divulgati, sin dall'emanazione della legge 31 dicembre 1996, n. 675 (poi abrogata e sostituita dal D.Lgs. n. 196/2003), ha visto ampliarsi il proprio contenuto venendo a compendiarsi anche del diritto alla protezione dei dati personali (Cass. 24 aprile 2008, n. 10690), il cui trattamento è soggetto a particolari condizioni (v. Cass. 25 maggio 2000, n. 6877).
Con il D.Lgs. n. 196/2003, il legislatore ha introdotto un sistema informato al prioritario rispetto dei diritti e delle libertà fondamentali e della dignità della persona, e in particolare della riservatezza e del diritto alla protezione dei dati personali nonché dell'identità personale o morale del soggetto (art. 2).
In tale quadro, imprescindibile rilievo assume il bilanciamento tra contrapposti diritti e libertà fondamentali, dovendo al riguardo tenersi conto del rango di diritto fondamentale assunto dal diritto alla protezione dei dati personali, tutelato agli artt. 21 e 2 Cost., nonché all'art. 8 Carta dei diritti fondamentali dell'Ue, quale diritto a mantenere il controllo sulle proprie informazioni che, spettando a "chiunque" (art. 1, D.Lgs. n. 196/2003) e ad "ogni persona" (art. 8 Carta), nei diversi contesti ed ambienti di vita, "concorre a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza" (così Cass., 4 gennaio 2011, n. 186 dell'Ue).
Il D.Lgs. n. 196/2003, ha pertanto sancito il passaggio da una concezione statica a una concezione dinamica della tutela della riservatezza, tesa al controllo dell'utilizzo e del destino dei dati.
Il soggetto interessato è divenuto compartecipe nell'utilizzazione dei propri dati personali.
I dati personali oggetto di trattamento debbono essere: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
La liceità del trattamento trova fondamento anche nella finalità del medesimo, quest'ultima costituendo un vero e proprio limite intrinseco del trattamento lecito dei dati personali, che fonda l'attribuzione all'interessato del potere di relativo controllo (tanto con riferimento alle finalità originarie che ai successivi impieghi), con facoltà di orientarne la selezione, la conservazione e l'utilizzazione.
L'interessato ha diritto a che l'informazione oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale (c.d. principi di proporzionalità, pertinenza e non eccedenza) (art. 11, D.Lgs. n. 196/2003). Gli è pertanto attribuito il diritto di conoscere in ogni momento chi possiede i suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la can-

cellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione (art. 7, D.Lgs. n. 196/2003).
Al di là delle specifiche fonti normative, è in ogni caso il principio di correttezza (quale generale principio di solidarietà sociale - che trova applicazione anche in tema di responsabilità extracontrattuale - in base al quale il soggetto è tenuto a mantenere nei rapporti della vita di relazione un comportamento leale, specificantesi in obblighi di informazione e di avviso, nonché volto alla salvaguardia dell'utilità altrui - nei limiti dell'apprezzabile sacrificio -, dalla cui violazione conseguono profili di responsabilità in ordine ai falsi affidamenti anche solo colposamente ingenerati nei terzi (cfr. Cass. 20 febbraio 2006, n. 3651; 27 ottobre 2006, n. 23273; 15 febbraio 2007, n. 3462; 13 aprile 2007, n. 8826; 24 luglio 2007, n. 16315; 30 ottobre 2007, n. 22860; 27 aprile 2011, n. 9404; 19 agosto 2011, n. 17685; 5 aprile 2012, n. 5525; 28 aprile 2015, n. 17756; S.U., 25 novembre 2008, n. 28056) a fondare in termini generali l'esigenza del bilanciamento in concreto degli interessi, e, conseguentemente, il diritto dell'interessato ad opporsi al trattamento, quand'anche lecito, dei propri dati.
Se l'interesse pubblico sotteso al diritto all'informazione (art. 21 Cost.) costituisce un limite al diritto fondamentale alla riservatezza (artt. 21 e 2 Cost.), al soggetto cui i dati pertengono è correlativamente attribuito il diritto all'oblio (v. Cass. 9 aprile 1998, n. 3679; 26 giugno 2013, n. 16111; 24 giugno 2016, n. 13161), e cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati.
Atteso che il trattamento dei dati personali può avere ad oggetto anche dati pubblici o pubblicati (Cass. 25 giugno 2004, n. 11864), il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità.
Ai sensi dell'art. 11, comma 1, lett. *b)*, D.Lgs. n. 196/2003, i dati raccolti e trattati per una determinata finalità possono essere in effetti successivamente utilizzati per altri scopi, con la prima compatibili. Anche in tale ipotesi essi debbono essere peraltro trattati in modo lecito e secondo correttezza (art. 11, comma 1, lett. *c)*, D.Lgs. n. 196/2003) nonché conservati in forma che consenta l'identificazione del soggetto cui gli stessi pertengono per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e trattati (art. 11, comma 1, lett. *e)*, D.Lgs. n. 196/2003).

Decisione della Cassazione

Disattendendo la doppia conforme di merito, nel decidere la vertenza, con la sentenza n. 22313/2016, la sezione lavoro, ha accolto il ricorso datoriale, affermando che è legittimo il licenziamento del lavoratore che conserva files e materiale pornografico nel computer d'ufficio e che procede alla cancellazione dell'intero disco rigido al fine di evitare rilievi a seguito di ispezione aziendale.
In particolare, la Corte di cassazione, ha ritenuto il primo motivo di ricorso fondato nei sensi di seguito indicati.
Al riguardo, occorre premettere che il giudice del riesame, esaminando la contestazione che aveva ad oggetto la cancellazione del disco O dal computer effettuata dal dipendente al fine di evitare il controllo dello stesso nel corso dell'ispezione, ha valorizzato la scusabilità del comportamento del dipendente, determinato dalle "modalità abusive" con le quali quella si sarebbe svolta, come riassunte nello storico di lite, tra cui l'apertura dei files pubblicamente.
Tale contesto sollecita a chiarire che la Suprema Corte fa rilevare in primis che il motivo non attiene alla materia dei c.d. controlli a distanza disciplinati dall'art. 4, Statuto dei lavoratori, rubricato "Impianti audiovisivi", né all'utilizzo dei dati desunti dal computer aziendale, ma del controllo da parte del datore di lavoro sull'utilizzo dello strumento presente sul luogo di lavoro e in uso al lavoratore per lo svolgimento della prestazione.
La norma richiamata (poi modificata con effetto dal 24 settembre 2015 dal D.Lgs. 14 settembre 2015, n. 151 - Jobs Act), sancisce al comma 1 che è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a di-

stanza dell'attività dei lavoratori. Lo stesso articolo, tuttavia, al comma 2, prevede che esigenze organizzative, produttive ovvero di sicurezza del lavoro possano richiedere l'eventuale installazione di impianti ed apparecchiature di controllo, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso è prevista una garanzia procedurale a vari livelli, essendo l'installazione condizionata all'accordo con le rappresentanze sindacali aziendali o con la commissione interna, ovvero, in difetto, all'autorizzazione dell'Ispettorato del lavoro.

Da questa premessa ne deriva più precisamente che la questione sottoposta all'attenzione della Cassazione 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".

La sezione lavoro della Cassazione ha stabilito al riguardo (v. sentenza 23 febbraio 2012, n. 2722), 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 (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).

Nel caso in disamina la condotta del lavoratore oggetto del controllo ispettivo 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.

Per altro verso, va rilevato che la giurisprudenza di legittimità - v. Cass. 17 luglio 2007, n. 15982 - ha avuto altresì modo di chiarire che l'art. 4 dello Statuto dei lavoratori "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". Con questa stessa sentenza, è stato però precisato che la "insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore", per cui "tale esigenza" "non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbliga-

zioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso".
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. È stato precisato che in tal caso si è di fronte a "un controllo c.d. 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).
Del resto, come già affermato da Cass. 18 febbraio 1983, n. 1236, l'articolo in esame "disciplina distintamente le due ipotesi" delle apparecchiature finalizzate al controllo a distanza dell'attività dei lavoratori (comma 1) e delle apparecchiature richieste da esigenze organizzative e produttive ovvero della sicurezza del lavoro, "ma tali comunque da presentare la possibilità di fornire anche il controllo a distanza del dipendente", le prime assolutamente vietate, le seconde consentite "soltanto a condizione che il datore di lavoro osservi quanto tassativamente previsto".
Riassumendo con Cass. 19 settembre 2016, n. 18302, l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che, anche per i c.d. controlli difensivi trovino applicazione le garanzie dell'art. 4, legge n. 300/1970 e che comunque questi ultimi, non si traducano in forme surrettizie di controllo a distanza dei lavoratori. Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche all'attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, comma 2, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le Rsa, si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che è vietato dall'art. 4, comma 1.

Conclusioni in merito ai controlli di sicurezza informatica

La Cassazione ha pertanto giudicato legittimo il licenziamento disciplinare del dipendente a seguito di controlli di sicurezza informatica sul computer in sua dotazione. La verifica operata da parte del datore di lavoro era avvenuta nel rispetto della privacy e della riservatezza del lavoratore, mentre la condotta del dipendente è risultata non accettabile anche per aver ostacolato la regolare esecuzione delle ispezioni.
Si è sopra già evidenziato che nel caso di specie la Corte d'Appello, esaminando la contestazione datoriale, ha valorizzato la scusabilità del comportamento del dipendente, determinato dalle modalità abusive con le quali la modalità di contestazione si sarebbe svolta, tra cui quella di pretendere pubblicamente l'apertura dei files.
La premessa in diritto sopra esposta, dalla quale muove la Corte d'Appello (scusabilità del comportamento del dipendente), ad avviso della sezione lavoro è corretta. Ed infatti, ribadisce la Cassazione 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 p.c. aziendali.
Nell'esercizio di tale prerogativa, sottolinea la sentenza n. 22313/2016 in esame, 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.
In altri termini, i controlli mirati all'osservanza della policy aziendale devono rispettare i principi di correttezza, pertinenza e non eccedenza *ex* art. 11, comma 1, Codice privacy, mentre le ispezioni sulle dotazioni di lavoro possono comunque determinare il trattamento di informazioni personali o dati sensibili non pertinenti all'indagine.
Ciò, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile (cfr. sul punto Cass. 5 aprile 2012, n. 5525; 1° agosto 2013, n. 18443).

Pertanto, conclude la Cassazione nel caso in esame distaccandosi dall'assunto della sentenza impugnata, che alla pur valida premessa di diritto assunta dalla Corte d'Appello, doveva seguire il controllo fattuale in ordine alle concrete modalità con le quali l'ispezione era stata condotta, onde accertare la reale consistenza delle attività effettuate e delle richieste degli ispettori, nonché la loro conformità con eventuali policy aziendali, cosa che però non vi è stata.
Da qui l'errore di valutazione della Corte territoriale che ha dato per pacifiche tali modalità invasive della privacy, confermando la ricostruzione secondo cui gli ispettori dell'azienda avevano preteso di aprire pubblicamente i files personali.
Sul punto ha dunque peccato il giudice del riesame, che nell'assunzione di detta determinazione non ha, invece, richiamato - come era suo onere - le fonti del proprio convincimento e malgrado lo specifico motivo di appello formulato in proposito dalla datrice di lavoro e "le dissonanti deduzioni e capitolazioni istruttorie". Lo stesso va detto riguardo all'affermazione secondo la quale i dati cancellati dal sottoposto erano integralmente recuperabili sul server aziendale.
Si può quindi concludere sul punto richiamando l'analogo principio di diritto affermato da Cass. 8 novembre 2016, n. 22662: "Non è soggetta alla disciplina dell'art. 4, comma 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".

Valutazione atomistica della personalità del lavoratore

In questo contesto, la Suprema Corte ha accolto anche la lamentela datoriale in base al quale veniva dedotta violazione dell'art. 1326 c.c. in relazione all'affermazione della Corte d'Appello secondo cui il datore di lavoro avrebbe rinunciato a dare rilievo al potenziale rischio di coinvolgimento in un reato ai sensi del D.Lgs. 8 giugno 2001, n. 231 (sulla responsabilità amministrativa delle società e degli enti), mentre nella lettera di licenziamento la datrice di lavoro evidenziava l'avere il dipendente esposto la stessa ai rischi conseguenti l'acquisizione del proprio sistema informatico di file che potrebbero comportare un coinvolgimento e sanzioni ai sensi del D.Lgs. n. 231/2001, qualora i files scaricati avessero riguardato minorenni.
Inoltre, la ricorrente contesta la motivazione della Corte territoriale secondo cui l'azienda non potrebbe invocare il bilanciamento tra diritto alla privacy e diritto della datrice stessa a non incorrere in responsabilità per violazione della legge sulla privacy, avendo di fatto rinunciato nella lettera di licenziamento alla contestazione relativa al potenziale rischio discendente da tale violazione.
Argomentazioni, queste, che vengono anch'esse accolte dalla Suprema Corte, con la precisazione che non è vero che l'azienda ha rinunciato a dare rilievo al potenziale rischio di coinvolgimento in un reato *ex* "231", in quanto nella lettera di contestazione si legge espressamente che i contenuti dei file saranno "trasmessi all'organismo di vigilanza di cui al Decreto legislativo n. 231/2012 per il seguito che lo stesso vorrà dare".
Inoltre, sottolinea la sezione lavoro che il licenziamento veniva giustificato anche sulla base della considerazione che l'insubordinazione atta a contestare l'attività ispettiva era assommata "ad un profilo non specchiato che le contestazioni ulteriori evidenziano".
Queste motivazioni della contestazione della massima sanzione espulsiva, sostiene in conclusione la Suprema Corte, erano state valorizzate dalla datrice al fine della complessiva valutazione della personalità del lavoratore, aspetto che non risulta, invece, essere stato considerato dal giudice del gravame, asserragliato ad una valutazione meramente atomistica della questione.
Come è noto, infatti, in tema di sindacato del vizio della motivazione, il compito del giudice di legittimità non è quello di sovrapporre la propria valutazione a quella compiuta dal giudice di merito in ordine all'affidabilità delle fonti di prova, bensì di stabilire se nel giudizio di merito siano stati esaminati tutti gli elementi, se sia stata fornita una corretta interpretazione di essi e se siano state esattamente applicate le regole della logica nello sviluppo delle argomentazioni che hanno giustificato la scelta di affermare la responsabilità penale dell'imputato.

La sentenza

Cass. civ., sez. lav., 25 maggio - 3 novembre 2016, n. 22313 - Pres. Di Cerbo - Rel. Ghinoy

Svolgimento del processo

La Corte d'Appello di Venezia con la sentenza n. 255/2015, giudicando sul reclamo proposto *ex* art. 1, comma 58, legge n. 92/2012, confermava la sentenza del Tribunale della stessa sede che aveva dichiarato l'illegittimità del licenziamento intimato dalla Cassa di risparmio di X Spa a F.F., 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 files con estensione video contenuti nel disco O, cancellava l'intero contenuto del disco, rendendo impossibile dare seguito all'attività ispettiva. All'esito di un successivo esame dell'archivio informatico, era emersa la presenza di materiale con contenuto pornografico.
Alla luce di tutto ciò, gli si contestava di aver ostacolato l'attività ispettiva del servizio revisione, di avere violato l'obbligo di tenere una condotta informata ai principi di disciplina, dignità e moralità sia in sede di effettuazione delle attività di revisione, sia acquisendo e conservando nel computer aziendale materiale pornografico, di avere violato l'obbligo di dedicare il suo tempo lavorativo all'attività aziendale, di avere violato il codice di comportamento che prescrive che i dipendenti della cassa sono tenuti ad utilizzare le apparecchiature esclusivamente per finalità di ufficio, di aver esposto la cassa ai rischi conseguenti l'acquisizione nel proprio sistema informatico di files che potrebbero comportare un coinvolgimento e sanzioni ai sensi del Decreto legislativo n. 231/2001 ove il materiale fosse a coinvolgere i minorenni.
La Corte territoriale riteneva che il licenziamento fosse illegittimo per insussistenza del fatto contestato, considerato che la banca non aveva dimostrato l'esistenza di documenti di pertinenza aziendale all'interno della parte del disco fisso del pc che era stata cancellata dal lavoratore; inoltre, il comportamento doveva ritenersi senz'altro scusabile in considerazione del fatto che gli ispettori avevano travalicato i propri poteri, imponendo al lavoratore l'immediata visione dei files, con richiesta abusiva perché sproporzionata e tale da lederne la privacy. Il giudice di secondo grado riconosceva quindi la tutela prevista al comma IV, art. 18, legge n. 300/1970, come novellato dalla legge n. 92/2012, in luogo della tutela di cui al comma V applicata dal primo giudice. Disponeva la prosecuzione del giudizio per la quantificazione delle provvidenze spettanti: il giudizio veniva poi definito con la successiva sentenza n. 840/2014, che escludeva l'esistenza dell'*aliunde perceptum*.
Per la Cassazione delle due sentenze la Cassa di risparmio ha proposto ricorso, affidato a quattro motivi, illustrati anche con memoria *ex* art. 378 c.p.c., cui ha resistito con controricorso F.F.

Motivi della decisione

1. Preliminarmente, la Cassa di risparmio nella memoria *ex* art. 378 c.p.c. ha eccepito l'inammissibilità del controricorso in quanto notificato oltre il termine previsto dall'art. 370, comma 1 c.p.c.
L'eccezione è fondata: la notifica del ricorso (effettuata presso lo studio dell'avv. G.M. che risulta dall'intestazione della sentenza domiciliatario nel giudizio d'appello) si è perfezionata in data 15 giugno 2015, data in cui si è verificata la compiuta giacenza del plico non ritirato, come risulta dalla cartolina depositata. La notifica del controricorso è stata poi effettuata a mezzo posta dal difensore ai sensi dell'art. 1, legge n. 53/1994 e la spedizione è avvenuta in data 28 luglio 2015, quindi oltre termine indicato.
Il controricorso deve ritenersi dunque inammissibile, il che preclude il suo esame, ma non ha impedito la partecipazione del difensore della parte alla discussione orale (Cass. n. 9023/2005).
2. I motivi di ricorso possono essere così riassunti:
2.1. Con il primo, la Cassa attinge la motivazione della Corte d'Appello, laddove ha ritenuto che gli ispettori avrebbero ecceduto dai propri poteri, potendo rinviare ad un secondo momento la visione del files sospetti, conservati nel server, anziché procedere in presenza dei colleghi.
Tale affermazione viene censurata sotto un primo profilo per violazione e falsa applicazione dell'art. 6 Cedu e artt. 115 e 116 c.p.c. oltre che per omesso esame di un fatto decisivo per il giudizio. Sostiene la Cassa che la ricostruzione dei fatti posti dalla Corte d'Appello alla base della propria decisione non corrisponderebbe ai fatti dedotti e provati, in quanto gli ispettori non chiesero al ricorrente di aprire i files, ma si limitarono a chiedere informazioni al riguardo e, dopo che il dipendente ne aveva cancellati alcuni, lo avevano invitato a non cancellarne ulteriori in quanto ciò avrebbe costituito un ostacolo all'attività ispettiva. Inoltre, l'attività di backup del server non aveva garantito l'integrale conservazione del contenuto ed era stato possibile recuperare solo i files risalenti solo sino a due giorni prima dell'ispezione. Aggiunge che né il lavoratore né la relazione ispettiva avevano parlato della presenza all'ispezione di altri soggetti, a parte la direttrice intervenuta dopo la cancellazione del disco per intimare al lavoratore di non continuare con l'eliminazione. Riferisce di avere chiesto prova diretta e controprova su tali circostanze, non ammessa dai giudici di merito.

Sotto, un secondo profilo, le argomentazioni della Corte territoriale vengono censurate per violazione o falsa applicazione del Decreto legislativo 30 giugno 2003, n. 196 e dell'articolo 2104 c.c.; si sostiene che chi è chiamato a verificare il rispetto delle norme in materia di sicurezza informatica può apprendere il contenuto dei files che si trovano nello strumento informatico affidato dall'azienda al lavoratore, sicché la condotta di chi impedisca tale verifica deve essere qualificata come illegittima.

2.2. Come secondo motivo, la Cassa deduce violazione dell'articolo 1326 c.c. in relazione all'affermazione secondo cui la Banca avrebbe rinunciato a dare rilievo al potenziale rischio di coinvolgimento in un reato ai sensi del D.Lgs. n. 231/2001 e omesso esame di un fatto decisivo per il giudizio. Il motivo attinge la motivazione della Corte territoriale secondo cui la banca non potrebbe invocare il bilanciamento tra diritto alla privacy e diritto della banca a non incorrere in responsabilità per violazione del Decreto legislativo suddetto, avendo di fatto rinunciato nella lettera di licenziamento alla contestazione relativa al potenziale rischio discendente dalla violazione di tale Decreto legislativo.

2.3. Come terzo motivo, deduce violazione e falsa applicazione degli artt. 42 del codice penale e 1218 e 2043 del codice civile, per erronea esclusione della sussistenza di un'ipotesi di dolo, in quanto il comportamento del lavoratore sarebbe stato volto ad uscire dall'impasse e non a cancellare file rilevanti per la banca; violazione e falsa applicazione degli articoli 18 commi 4, 5 e 6, legge n. 300/1970, 2106 c.c., dal momento che l'applicazione dell'articolo 18, comma quattro (insussistenza del fatto materiale) apparirebbe contraddittoria con la rilevata qualifica di "scusabile" del comportamento posto in essere (quindi comportamento materialmente sussistente, ma soggettivamente scusabile). Per tale motivo chiede che in via subordinata, qualora il licenziamento venga ritenuto illegittimo, si dichiari l'applicabilità alla fattispecie dell'articolo 18 comma cinque e non già dell'articolo 18, comma quattro, legge n. 300/1970.

2.4. Come quarto motivo, deduce violazione e falsa applicazione degli articoli 18, commi 4, 5 e 6, legge n. 300/1970, 2106 c.c., 115 c.p.c. e lamenta l'omesso rilievo delle altre contestazioni oltre a quella relativa all'insubordinazione, violazione dell'articolo 1326 c.c. quanto all'interpretazione della lettera di licenziamento.

Riferisce che erano state mosse al lavoratore altre contestazioni oltre a quella più rilevante di insubordinazione, ritenute sussistenti dal giudice della prima fase, aventi ad oggetto il possesso di materiale pornografico in violazione della normativa aziendale che vietava l'utilizzo del computer per fini diversi da quelli lavorativi, nonché la sottrazione del tempo di lavoro l'attività lavorativa.

3. Il primo motivo di ricorso è fondato nei sensi di seguito indicati.

Occorre premettere che il motivo non attiene alla materia dei c.d. controlli a distanza disciplinati dall'art. 4, legge n. 300/1970, né all'utilizzo dei dati desunti dal computer aziendale, ma del controllo da parte del datore di lavoro sull'utilizzo dello strumento presente sul luogo di lavoro e in uso al lavoratore per lo svolgimento della prestazione.

La Corte d'Appello, esaminando la contestazione che aveva ad oggetto la cancellazione del disco O dal computer effettuata dal dipendente al fine di evitare il controllo dello stesso nel corso dell'ispezione, ha valorizzato la scusabilità del comportamento del dipendente, determinato dalle modalità abusive con le quali quella si sarebbe svolta, riassunte nello storico di lite, tra cui quella di pretendere pubblicamente l'apertura dei files.

3.1. La premessa in diritto dalla quale muove la Corte territoriale è corretta. Ed infatti 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 p.c. 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; ciò, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile (cfr. sul punto Cass. civ. 5 aprile 2012, n. 5525 e n. 18443 del 1° agosto 2013).

3.2. Nel caso, a tale premessa in diritto doveva quindi seguire il controllo fattuale in ordine alle concrete modalità con le quali l'ispezione era stata condotta, onde accertare la reale consistenza delle attività effettuate e delle richieste degli ispettori, nonché la loro conformità con eventuali policy aziendali.

Tali modalità invasive della privacy vengono date per pacifiche dalla Corte territoriale, che ha confermato la ricostruzione secondo la quale gli ispettori avevano preteso di aprire pubblicamente i files personali; ciò tuttavia ha fatto senza richiamare le fonti del proprio convincimento e malgrado lo specifico motivo di appello formulato in proposito dalla Banca (il primo, a p. 39 del reclamo, riportato a p. 12 del ricorso per cassazione) e le dissonanti deduzioni e capitolazioni istruttorie (riportate alle pagg. 20 e 21 del ricorso per cassazione). Lo stesso dicasi per l'affermazione secondo la quale i dati cancellati erano integralmente recuperabili sul server.

4. Analogamente fondato è il secondo motivo.

Nella lettera di contestazione si legge (p. 31 del ricorso): "Per quanto riguarda l'ultimo punto della contestazione (n.d.r., il punto e), afferente "l'aver esposto la Cassa ai rischi conseguenti l'acquisizione del proprio sistema informativo di file che potrebbero comportare un coinvolgimento e sanzioni ai sensi del Decreto legislativo n.

231/2001"), i contenuti verranno trasmessi all'organismo di vigilanza di cui al Decreto legislativo n. 231/2001 per il seguito che lo stesso vorrà dare".
Inoltre, la massima sanzione espulsiva veniva giustificata, come riferisce la stessa Corte d'Appello a p.. 14, anche sulla base delle considerazioni che l'insubordinazione atta a contestare l'attività ispettiva era assommata "ad un profilo non specchiato che le contestazioni ulteriori evidenziano".
4.1. Ne risulta pertanto che, nell'irrogazione del licenziamento, la Banca aveva valorizzato al fine della complessiva valutazione della personalità del lavoratore anche il punto e) della contestazione disciplinare, che invece non è stato considerato dal giudice del gravame.
5. Gli ulteriori motivi di ricorso, che attengono a questioni che possono rilevare solo una volta definita nei suoi contorni essenziali l'effettiva consistenza e natura della condotta addebitata quale risultata confermata all'esito del vaglio fattuale demandato al giudice di merito, restano assorbiti.
6. Segue la cassazione della sentenza impugnata ed il rinvio alla Corte d'Appello di Venezia in diversa composizione, per una nuova valutazione in relazione ai motivi accolti, ed anche per la liquidazione delle spese del presente giudizio.

P.Q.M.

La Corte accoglie il primo e secondo motivo di ricorso, assorbiti gli altri. Cassa la sentenza impugnata in relazione ai motivi accolti e rinvia, anche per le spese, alla Corte d'Appello di Venezia in diversa composizione.