22 SET. 2021

AULA 'A'

ESENTE REGISTRAZIONE ESENTE BOLLI ESENTE DIRITTI

25732/21

Oggetto

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

R.G.N. 16932/2019

SEZIONE LAVORO

Cron. 25732

[redacted]

SENTENZA

[redacted]

2021

2181

FATTI DI CAUSA

1. Con ricorso ai sensi dell'art. 1 comma 47 della legge 28 giugno 2012, n. 92, [redacted] impugnava dinanzi al Tribunale di Roma il licenziamento per giusta causa intimatole il 29 gennaio 2016 dalla Fondazione Accademia Nazionale di Santa Cecilia chiedendo che ne fosse accertata l'illegittimità e fosse disposta la sua reintegrazione nel posto di lavoro ai sensi dell'art. 18 della legge 20 maggio 1970 n. 300 e sue successive modificazioni. All'esito della fase sommaria il Tribunale rigettava il ricorso. In sede di opposizione veniva invece dichiarata l'illegittimità del recesso e disposta la reintegrazione della lavoratrice nel posto di lavoro.
2. In seguito all'accertamento della diffusione di un *virus* nella rete aziendale l'amministrazione del sistema informatico della Fondazione aveva eseguito un accesso sul *computer* della lavoratrice, appurando che nella cartella di *download* del disco fisso della [redacted] era presente un *file* scaricato che aveva propagato il *virus* che, partito dal *computer* aziendale in uso alla lavoratrice, aveva iniziato a propagarsi nella rete della Fondazione, criptando i *files* all'interno di vari dischi di rete, rendendo gli stessi illeggibili e quindi inutilizzabili. In occasione dell'intervento venivano in rilievo numerosi accessi – da parte della lavoratrice - a siti che all'evidenza erano stati visitati per ragioni private, per un tempo lungo, tale da integrare una sostanziale interruzione della prestazione lavorativa.
3. Con lettera del 30.11.2015 alla [redacted] veniva contestato, per il periodo 16.10.2015-16.11.2015:
   a) L'impiego di mezzi informatici messi a disposizione dal datore di lavoro per l'esecuzione della prestazione lavorativa a soli fini privati ed in violazione delle disposizioni impartite in ordine all'utilizzo degli stessi nonché dei più elementari doveri di diligenza, correttezza e buona fede nell'esecuzione dlela prestazione;
   b) la sostanziale interruzione in tutto il periodo di riferimento della prestazione lavorativa, visti tempi e quantità di navigazione per fini privati;
   c) l'aver causato con il suo operato gravi danni al patrimonio aziendale sia per la perdita dei dati sia per l'impossibilità degli uffici della Fondazione di accedere alle cartelle elettroniche danneggiate per tutto il tempo necessario al ripristino del sistema;
   d) La recidiva, tenuto conto dell'evenienza che, a fronte della contestazione disciplinare datata 26.11.2013, prot. n. 10323, le era stata applicata, in data

19.12.2013, prot. n. 1539, la sanzione del licenziamento per giusta causa, successivamente convertita in via transattiva in sospensione dal servizio.

4. Assunte le giustificazioni della lavoratrice, si giungeva al citato licenziamento.
5. Adita dalla lavoratrice con ricorso presentato *ex* art. 145 d.lgs. n. 196/2003, l'Autorità Garante per la Protezione dei Dati Personali, con delibera 12.10.2016, ordinava alla Fondazione di astenersi dall'effettuare qualsiasi ulteriore trattamento dei dati acquisiti dalla cronologia del *browser Google Chrome* del computer aziendale in uso alla ricorrente e relativi al periodo 16.10.2015-16.11.2015, "*... eccettuata la mera conservazione degli stessi ai fini della loro eventuale acquisizione da parte giudiziaria...*". Con sentenza n. 5987 del 28.3.2018 il Tribunale di Roma confermava tale delibera.
6. In sede di opposizione, il Tribunale – giudice del lavoro – riteneva:
   a) che la delibera dell'Autorità Garante non ostava alla utilizzazione nel processo dei dati estratti dal computer aziendale in uso alla lavoratrice, non operando un regime di "giudicato" per le pronunce dell'Autorità ed anzi avendo il predetto Ufficio affermato che i dati in questione erano conservabili dalla parte datoriale a fini di difesa in giudizio;
   b) che l'acquisizione dei predetti dati non si era risolta in un controllo a distanza vietato dall'art. 4 l. n. 300 del 1970, perché la verifica del datore di lavoro è stata finalizzata a bonificare il sistema informatico della Fondazione dal *virus* che ne poneva in pericolo il funzionamento, senza alcun intento di sorvegliare l'adempimento della prestazione lavorativa dovuta dalla [redacted];
   c) che, tuttavia, il comportamento della lavoratrice non aveva esposto la Fondazione al rischio dell'applicazione di una sanzione prevista dal d.lgs. n. 231/2001, e, tenuto conto di vari fattori, come la non assoluta incompatibilità con le mansioni della lavoratrice degli accessi riscontrati, la loro parziale esecuzione in orario notturno e il difetto di contestazioni da parte datoriale di mancato rispetto da parte delle lavoratrice di termini o incombenze di lavoro arretrato, o la sussistenza di lavoro, non si poteva ritenere che lo stesso comportamento avesse leso irreparabilmente il rapporto di fiducia con l'ente non consentendo la prosecuzione neanche provvisoria del rapporto di lavoro, il licenziamento si doveva ritenere sproporzionato alle mancanze riscontrate, per cui veniva accordata la tutela reintegratoria prevista dall'art. 18 della legge n. 300 del 1970 nel testo antecedente all'entrata in vigore della l. n. 92/2012.

7. Investita del reclamo della Fondazione e di quello incidentale della Ciamarra, la Corte di appello di Roma, in riforma della sentenza del Tribunale, rigettava il ricorso introduttivo proposto dalla [redacted] che condannava al pagamento delle spese di entrambi i gradi del giudizio.
8. La Corte territoriale ha ritenuto, sul punto non discostandosi dalle conclusioni del Tribunale, che i dati che la Fondazione aveva acquisito dal *browser Google Chrome* del computer aziendale in uso alla [redacted] relativi al periodo 16.10-16.11.2015, potevano essere conservati "ai fini della loro eventuale acquisizione da parte dell'autorità giudiziaria" e, perciò, legittimamente erano stati utilizzati a tale fine nel giudizio.
9. La stessa Corte ha escluso che fosse configurabile la violazione dell'art. 4 dello Statuto dei lavoratori atteso che, come già accertato dal Tribunale, il controllo sul *computer* aziendale della [redacted] si era reso necessario per verificare l'origine del *virus* che aveva infettato il sistema informatico della Fondazione criptando dati e causandone in parte irrimediabilmente la perdita. Ha ritenuto corretta la ricostruzione dei fatti operata dal Tribunale evidenziando che il giudice dell'opposizione aveva ritenuto sproporzionata la sanzione irrogata.
10. Diversamente dal giudice dell'opposizione, però, la Corte di merito ha ritenuto che l'ingente numero di accessi ad *internet* aveva natura ludica e privata. Inoltre ha posto in rilievo che non era stata provata la sincronizzazione con il computer aziendale di dispositivi mobili, così svalutando il rilievo dell'ora notturna alla quale erano stati eseguiti alcuni accessi, circostanza che era stata dal Tribunale valutata in favore della lavoratrice, e che dai numerosi accessi ad *internet* per fini personali era risultata frammentata la prestazione lavorativa resa in maniera discontinua, in modo da svilire la qualità dei compiti a lei affidati. Ha poi ritenuto provata l'intenzionalità della condotta e proporzionata la sanzione in relazione alla avvenuta violazione dell'art. 33 del c.c.n.l. applicato dalla Fondazione. Ha accertato infatti che con il suo comportamento la lavoratrice aveva consapevolmente trasgredito alle indicazioni date dalla Fondazione con riguardo all'uso degli strumenti informatici, indicazioni delle quali era stata compiutamente resa edotta, così sottraendo energie alla prestazione lavorativa ed incrinando irrimediabilmente la fiducia datoriale in relazione alla correttezza del futuro adempimento della prestazione, tenuto conto anche della sanzione disciplinare già irrogatale nel 2013 per una violazione che presentava analogie con quella contestata corroborando la valutazione di gravità della condotta.

11. Per la cassazione della sentenza ricorre [redacted] che articola tre motivi ai quali resiste con controricorso la Fondazione Accademia Nazionale di Santa Cecilia. Entrambe le parti hanno depositato memoria.
12. Inizialmente fissata alla pubblica udienza del 5 marzo 2020, la discussione del ricorso veniva rinviata a nuovo ruolo, e rifissata all'udienza odierna, in considerazione della novità e del rilievo nomofilattico delle questioni relative all'interpretazione del novellato art. 4 della legge n. 300 del 1970 e considerata l'opportunità della trattazione in un'unica udienza degli altri ricorsi pendenti che investono analoghe questioni.
13. Il Procuratore Generale presso questa Corte ha depositato conclusioni scritte ai sensi dell'art. 23, comma 8-*bis*, d.l. n. 137/2020, conv, in l. n. 176/2020, concludendo per il rigetto del ricorso.

RAGIONI DELLA DECISIONE

1. Preliminarmente si osserva che in memoria la parte ricorrente ha richiesto, in considerazione della complessità e della novità delle questioni sollevate in ricorso, la rimessione della trattazione del ricorso alle Sezioni Unite di questa Corte ai sensi dell'art. 376 cod.proc.civ. Non ritiene la Corte opportuno, a questo stadio, l'intervento del Supremo Collegio.
2. Con il primo motivo di ricorso è denunciata la violazione e falsa applicazione dell'art. 2119 cod. civ. dell'art. 4 della legge 20 maggio 1970 n. 300, dell'art. 160 comma 6 del Codice della *privacy*, dell'art. 2702 e ss. cod. civ. e degli artt. 115 e 245 cod. proc. civ. per avere ritenuto utilizzabili a fini disciplinari e comunque dimostrabili le informazioni acquisite in violazione dei diritti di informativa e dei diritti stabiliti dal codice della *privacy*.
3. Sostiene la ricorrente che la datrice di lavoro, la quale aveva acquisito la cronologia dei dati di accesso ad *internet* dalla postazione della [redacted] in occasione della ricerca di un *virus* informatico, non avrebbe potuto utilizzare tali dati a fini disciplinari in quanto, in assenza di un'adeguata informazione alla lavoratrice delle modalità di effettuazione dei controlli, l'ulteriore utilizzo per i fini connessi al rapporto di lavoro ne è precluso.
4. Evidenzia inoltre la lavoratrice che con ordinanza del Tribunale di Roma, davanti al quale era stato impugnato il provvedimento dell'Autorità Garante per la Protezione dei Dati Personali, era stata confermata l'avvenuta violazione degli obblighi di informativa regolati anche dal d.lgs. n.196 del 2003 e l'eccedenza del

trattamento rispetto alle sue finalità ed era stato intimato alla datrice di lavoro di astenersi dall'effettuare qualsiasi ulteriore trattamento dei dati acquisiti e relativi al periodo 15.10 - 15.11.2015. L'inutilizzabilità delle informazioni si riverbera ad avviso della ricorrente sul piano della prova dell'illecito disciplinare che sarebbe stata illegittimamente acquisita

5. Ritiene la ricorrente che la completa irrilevanza giuridica del fatto equivale alla sua insussistenza materiale (cfr. Cass. 20540/2015), giacché non può essere provato ciò che si fonda su informazioni non utilizzabili. La preclusione di cui all'art. 4 comma 3 opera sull'utilizzabilità dell'informazione.
6. Con il secondo motivo di ricorso è denunciata la violazione e falsa applicazione dell'art. 2119 cod. civ., dell'art. 18 comma 4 legge 20 maggio 1970 n. 300 nonché degli artt. 1362,1363, 1364 e 1365 cod.civ. e dell'art. 1370 cod. civ. con riguardo alle disposizioni del codice etico e del sistema disciplinare dell'Accademia di Santa Cecilia che prevedono l'applicazione di sanzioni espulsive sulla base di una graduazione di mancanze da gravi a gravissime legate anche all'esistenza di danni per l'ente. Nel caso in cui si ritenga ammissibile l'utilizzo delle informazioni acquisite in violazione dei limiti dell'art. 4 della legge n. 300 del 1970 la Corte di merito non avrebbe potuto distaccarsi dalla tipizzazione degli illeciti contenuta nel codice etico e nel sistema disciplinare. Se correttamente interpretata la condotta avrebbe potuto essere punita, al più, con una sanzione conservativa (sanzione della sospensione fino a cinque o fino a dieci giorni) trattandosi di svolgimento di attività ludiche durante l'orario di lavoro senza che ne sia stato arrecato un grave danno al patrimonio aziendale. Evidenzia la lavoratrice che per il licenziamento per giusta causa è necessario che la condotta violi una o più regole o principi previsti dal Modello, Codice Etico, Protocolli e dagli obblighi informativi dell'organismo di vigilanza tale da esporre l'Accademia al rischio di una sanzione prevista dal d.lgs. n. 231 del 2001 e da ledere irreparabilmente il vincolo fiduciario. Tanto premesso la ricorrente sottolinea che la condotta accertata non espone al rischio di sanzione prevista dal d.lgs. n. 231 del 2001 che prevede reati assai più gravi quali il peculato, la corruzione, la pedopornografia etc. Al contrario la sanzione conservativa della sospensione fino a dieci giorni è irrogata nel caso in cui sussista un danno patrimoniale e persino nel caso di esposizione ad una situazione oggettiva di pericolo. Erroneamente, perciò, la Corte di merito prescindendo dalla valutazione di proporzionalità effettuata dalla previsione contrattuale avrebbe irrogato il licenziamento per una

condotta punita con una sanzione conservativa. Né avrebbe rilievo il richiamo ad un precedente risalente nel tempo ai fini della valutazione della gravità della condotta. La recidiva può incidere solo nella misura in cui sia prevista nella condotta tipizzata (richiama Cass. 6165 del 2016 e 13787/2016).

7. Con il terzo motivo di ricorso è denunciata la violazione dell'art. 112 cod. proc. civ., degli artt. 1362, 1363, 1364 e 1365 cod.civ. e degli artt. 347 cod.proc.civ. con riferimento alla eccezione di tardività della sanzione sospensiva di 10 giorni applicata alla [redacted] La Corte territoriale avrebbe erroneamente interpretato la memoria difensiva in appello con la quale era stata denunciata la tardività e inutilizzabilità ai fini della recidiva della sanzione conservativa applicata in esito ad un accordo intervenuto tra le parti in occasione di un precedente procedimento disciplinare ed avrebbe trascurato di pronunciare sui rilievi con tale memoria formulati così incorrendo nelle violazioni denunciate.
8. Il primo motivo pone il tema, di indubbio rilievo nomofilattico, della compatibilità dei c.d. "controlli difensivi", concetto elaborato dalla giurisprudenza precedentemente alla modifica dell'art. 4 dello Statuto dei lavoratori recata dall'art. 23 del d.lgs. n. 151 del 2015 (uno dei decreti del c.d. *Jobs Act*) e dall'art. 5 d.lgs. n. 185 del 2016, con l'attuale assetto normativo. È dall'inquadramento in questa categoria dei controlli effettuati dalla Fondazione resistente, cioè della raccolta dei dati estratti dal *computer* in uso alla ricorrente, della loro conservazione e della loro utilizzazione in sede disciplinare che la Corte territoriale ha fatto discendere l'inapplicabilità alla fattispecie dell'art. 4 citato nella sua attuale versione, astrattamente applicabile *ratione temporis*.

I "controlli difensivi" prima della modifica dell'art. 4 St. lav.

9. L'originaria versione dell'art. 4 St.lav. (recante "Impianti audiovisivi") disponeva: "1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. 2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. 3. Per gli impianti e le apparecchiature esistenti, che rispondano alle

caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. 4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale".

10. La norma contemplava, in sostanza, due livelli di protezione della sfera privata del lavoratore: uno pieno, mediante la previsione del divieto assoluto di uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori non sorretto da ragioni inerenti all'impresa (ossia, il cd. controllo fine a sé stesso); l'altro affievolito, ove le ragioni del controllo fossero state riconducibili ad esigenze oggettive dell'impresa, ferma restando l'attuazione del controllo stesso con l'osservanza di determinate "procedure di garanzia".

11. Quanto alla *ratio*, la giurisprudenza di questa Corte ha evidenziato, da un lato, che la disposizione statutaria 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. Si è altresì precisato, d'altro canto, che la garanzia procedurale prevista per impianti ed apparecchiature ricollegabili ad esigenze produttive contempera l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro, o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi (Cfr., per tutte, Sez. L, 17 luglio 2007, n. 15892, in motivazione, sulla scorta di Sez. L, 17 giugno 2000,

n. 8250, del pari in motivazione, richiamata, sul punto, in quasi tutte le sentenze successive vertenti sul tema).

12. Questione centrale, dal punto di vista del tema che oggi occupa la Corte, era verificare se l'esigenza di tutela del patrimonio aziendale potesse esonerare il datore di lavoro intenzionato ad installare apparecchiature di controllo a distanza indipendentemente dalla necessità di ottenere l'accordo sindacale o l'autorizzazione amministrativa.

13. Pur potendo, infatti, tale esigenza rientrare, teoricamente, in quella "produttiva", essendo chiaro che la produttività dell'azienda si fonda sui risultati del lavoro - annientati ove, ad esempio, si verifichi una appropriazione di denaro in cassa ad opera del preposto - e sugli investimenti - verosimilmente vanificati ove i beni aziendali siano danneggiati o gli strumenti di lavoro sottratti -, era forte la convinzione che la legittimazione del datore di lavoro a proteggere il proprio patrimonio da attacchi "esterni" non potesse subire compressione a fronte di eventuali attacchi provenienti dall'interno (non poco insidiosi, in quanto verificabili con maggior frequenza in ambito lavorativo), tenuto conto dei poteri insiti nella titolarità dell'impresa.

14. D'altra parte, sembrava difficilmente accettabile l'idea che l'attuazione - quanto a modalità e tempi, necessariamente rapidi - di misure strategiche intese ad un controllo avente finalità meramente conservativa dovesse essere il frutto di una negoziazione, dagli esiti eventualmente incerti, o di una autorizzazione non priva di vincoli e condizioni tali da impoverire l'iniziativa messa in campo dal datore.

15. La giurisprudenza di questa Corte ha quindi elaborato, onde consentire al datore di lavoro di contrastare comportamenti illeciti del personale, la categoria dei c.d. "controlli difensivi".

16. Secondo l'indirizzo giurisprudenziale più recente e più evoluto, «esulano dall'ambito di applicazione dell'art. 4, comma 2, St. lav. (nel testo anteriore alle modifiche di cui all'art. 23, comma 1, del d.lgs. n. 151 del 2015) e non richiedono l'osservanza delle garanzie ivi previste, i "controlli difensivi" da parte del datore se diretti ad accertare comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale, tanto più se disposti *ex post*, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa. (Nella specie, è stata ritenuta legittima la verifica successivamente disposta sui dati relativi alla navigazione in

internet di un dipendente sorpreso ad utilizzare il computer di ufficio per finalità extralavorative)» (Cass., 28 maggio 2018, n. 13266).

17. In altri termini, i controlli datoriali a distanza, detti "difensivi", non erano assoggettati ai presupposti di legittimità stabiliti dal previgente art. 4, secondo comma, St.lav. in presenza di due condizioni necessarie e di una eventuale.

18. Era in primo luogo indispensabile che l'iniziativa datoriale avesse la finalità specifica di accertare determinati comportamenti illeciti del lavoratore. A tale ultimo riguardo poteva porsi il problema su come potesse adeguatamente esercitarsi il sindacato giudiziale sulla effettività (nonché veridicità) della finalità perseguita (ben potendo accadere che il datore esercitasse il controllo sull'attività lavorativa al di fuori di ogni garanzia e, per così dire, "a pioggia", ossia sulla generalità dei dipendenti, sul presupposto, meramente affermato, di voler accertare la commissione di determinati illeciti ad opera di un singolo lavoratore).

19. L'altro presupposto necessario era che gli illeciti da accertare fossero lesivi del patrimonio o dell'immagine aziendale (Cfr., tra le altre, Sez. L, 23 febbraio 2012, n. 2722, cit., che ha 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; ciò sul rilievo che esula dal campo di applicazione dell'art. 4, comma 2, St.lav., nella sua originaria versione, 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).

20. Il terzo presupposto era che i controlli fossero stati disposti *ex post*, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa; la sussistenza di tale presupposto offre plausibile attestazione della veridicità dell'intento datoriale, che, diversamente, non sarebbe, quale elemento facente parte della sfera interna del datore, agevolmente sindacabile (Cfr., al riguardo, Cass., 5 ottobre 2016, n. 19922, che ha ritenuto illegittimo il controllo effettuato mediante GPS installato sulle vetture in uso ai lavoratori, in quanto predisposto *ex ante* ed in via generale ben prima che si potessero avere sospetti su una eventuale violazione da parte del lavoratore licenziato.

21. Tale presupposto era però da considerare come eventuale, poiché ritenuto, per lo più, dalla giurisprudenza un fattore avente funzione meramente confermativa

della effettività del controllo difensivo; pertanto esso poteva mancare, essendo sufficiente il mero sospetto circa l'esecuzione di illeciti, quale ulteriore requisito di legittimità del controllo difensivo, senza che la natura difensiva del controllo venisse in astratto meno (salvo il problema di accertare, per altre vie, la esclusiva destinazione di esso all'accertamento di determinati illeciti; cfr., *mutatis mutandis*, Cass. 14 febbraio 2011, n. 3590).

22. Sebbene i "controlli difensivi" fossero sottratti all'area di operatività dell'originaria versione dell'art. 4, comma 2, St. lav., era chiaro nella giurisprudenza che essi non potevano comunque essere esercitati liberamente dal datore di lavoro al di fuori di regole di civiltà e di criteri ragionevoli volti a garantire, con l'impiego di determinati accorgimenti e cautele, un adeguato bilanciamento tra le esigenze di salvaguardia della dignità e riservatezza del dipendente e quelle di protezione, da parte del datore di lavoro, dei beni (in senso lato) aziendali.

23. Sicché la disciplina dei controlli in questione è stata ricostruita mediante il richiamo ai principi di *buona fede e correttezza* (cfr. Cass. 27 maggio 2015, n. 10955, in motivazione, secondo cui deve restare ferma «*la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l'interesse del datore di lavoro al controllo ed alla difesa della organizzazione produttiva aziendale deve contemperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale*»., *di proporzionalità e pertinenza* (cfr., sulla proporzionalità: Cass. 18 luglio 2017, n. 17723 secondo cui: «*Sono invasivi i controlli cd. difensivi, sotto l'aspetto temporale, eccedenti i limiti della adeguatezza e proporzionalità e, sotto il profilo sostanziale, indebitamente ricadenti sugli aspetti privati e personali estranei all'oggetto e al fine dell'indagine*».; sulla pertinenza: Cass. 10 novembre 2017, n. 26682, in motivazione, secondo cui : «*Pertanto, considerato che (...) il controllo era del tutto svincolato dall'attività lavorativa ed era stato effettuato per verificare se la strumentazione aziendale in dotazione fosse stata utilizzata per la perpetrazione di illeciti; che esso, al di fuori di una verifica preventiva a distanza dell'attività dei lavoratori, era stato occasionato da una anomalia di sistema tale da ingenerare il ragionevole sospetto dell'esistenza di condotte vietate e, quindi, giustificato dal motivo legittimo di tutelare il buon funzionamento dell'impresa nonché i dipendenti che vi lavorano, anche al fine di evitare di esporre l'azienda a responsabilità derivanti da attività illecite compiute in danno di terzi; che*

l'acquisizione dei dati era stata effettuata con modalità non eccedenti rispetto alle finalità del controllo e, quindi, nell'osservanza dei criteri di proporzionalità, correttezza e pertinenza, che non sono stati rilevati elementi dai quali desumere che il datore di lavoro avrebbe potuto utilizzare misure e metodi meno invasivi per raggiungere l'obiettivo perseguito (...)».anche ricavabili da disposizioni contenute nel "Codice Privacy".), nonché nel quadro della normativa europea ; sì da potersi affermare la illegittimità di un controllo difensivo attuato, comunque, in contrasto con detti principi.

La questione della "sopravvivenza" dei "controlli difensivi" nel regime normativo fissato dalla nuova formulazione dell'art. 4 St. lav.

24. L'art. 23 del d.lgs. 14 settembre 2015, n. 151 , prevede, per quanto qui interessa: "1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente: «Art. 4 (Impianti audiovisivi e altri strumenti di controllo). - 1. 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 e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. 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. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente 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. 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.»".

25. L'art. 5, comma 2, del d.lgs. 24 settembre 2016, n. 185, dispone: "All'articolo 4, comma 1, della legge 20 maggio 1970, n. 300 il terzo periodo è sostituito dai seguenti: «In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle (*recte*: "della") sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi»".
26. La norma ribadisce implicitamente la regola che il controllo a distanza dell'attività dei lavoratori non è legittimo ove non sia sorretto dalle esigenze indicate dalla norma stessa. Sicché il controllo "fine a sé stesso", eventualmente diretto ad accertare inadempimenti del lavoratore che attengano alla effettuazione della prestazione, continua ad essere vietato. Ciò non esclude, però, come si era ritenuto con riguardo alla superata disposizione dell'art. 4 St.lav., che ove il controllo sia invece legittimo, le informazioni raccolte in esito ad esso possano essere utilizzate dal datore di lavoro per contestare al lavoratore ogni sorta di inadempimento contrattuale.
27. La giurisprudenza di merito e la dottrina si sono poste la questione della eventuale sopravvivenza dei c.d. "controlli difensivi" dopo la modifica dell'art. 4 St. lav. ad opera dell'art. 23 del d.lgs. n. 151/2015. Né dall'una né dall'altra sono venute risposte univoche.
28. Va subito evidenziato, a tale riguardo, che i controlli aventi ad oggetto il patrimonio aziendale sono, ai sensi della nuova versione dell'art. 4 St.lav., assoggettati ai presupposti di legittimità ivi previsti, per cui si pone la questione se i "controlli difensivi" non debbano oramai ritenersi completamente attratti nell'area di operatività dell'art. 4 St. lav., avendo il legislatore indicato, tra le esigenze da soddisfare mediante l'impiego dei dispositivi potenzialmente fonte di controllo, accanto a quelle organizzative e produttive e a quelle relative alla sicurezza del lavoro, per l'appunto quelle di "tutela del patrimonio aziendale", ovvero se anche sotto l'impero della nuova versione dell'art. 4 St. lav. debba continuare a riconoscersi ai "controlli difensivi" diritto di cittadinanza.
29. Ritiene la Corte che possa soccorrere in questo contesto la distinzione tra i "controlli difensivi" in senso lato e quelli in senso stretto.
30. Si è osservato che la giurisprudenza ammissiva dei "controlli difensivi" nella vigenza del vecchio testo dell'art. 4 St. lav, e quindi della legittimità del controllo

anche in assenza del preventivo accordo sindacale o dell'autorizzazione amministrativa, dato che oggetto del controllo sarebbe stata non già l'attività lavorativa, bensì l'illecito commesso durante la prestazione lavorativa, derivava da quella che ammette, ai sensi dell'art. 3 St. lav., i controlli occulti tramite agenzie investigative diretti ad accertare condotte penalmente rilevanti dei lavoratori in occasione della prestazione (Cass., 22 maggio 2017, n. 12810; Cass., 4 dicembre 2014, n. 25674; Cass., 4 marzo 2014, n. 4984). Se ne è tratta la conclusione che questa tesi sembra difficilmente armonizzabile con la disciplina dei controlli tecnologici contenuta nell'art. 4 proprio per le modalità di funzionamento di tali controlli. A differenza di un incarico ad un'agenzia investigativa, che può essere limitato ai soli accertamenti necessari ad verificare l'eventuale illecito del singolo dipendente ed essere ritenuto legittimo proprio perché così circoscritto, l'impiego di controlli tecnologici attraverso un sistema informatico che tenga traccia di tutti i dati relativi all'attività di lavoro svolta dall'insieme dei dipendenti sarebbe privo di ogni selettività e non sarebbe ammissibile, perché non orientato specificamente sull'attività illecita, ma in modo indifferenziato sulle prestazioni rese da tutti i lavoratori.

31. Occorre perciò distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti e "controlli difensivi" in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro.
32. Si può ritenere che questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situino, anche oggi, all'esterno del perimetro applicativo dell'art. 4.
33. In effetti, come è stato osservato, l'istituzionalizzazione della procedura richiesta dall'art. 4 per l'installazione dell'impianto di controllo sarebbe coerente con la necessità di consentire un controllo sindacale, e, nel caso, amministrativo, su scelte che riguardano l'organizzazione dell'impresa; meno senso avrebbe l'applicazione della stessa procedura anche nel caso di eventi straordinari ed eccezionali costituiti dalla necessità di accertare e sanzionare gravi illeciti di un singolo lavoratore.

34. Questa soluzione è stata accolta da parte della giurisprudenza di merito, ad esempio dal Tribunale di Roma con la sentenza 24 marzo 2017, in *Diritto delle relazioni industriali,*, 2018, II, 265, secondo cui *«È legittimo il controllo c.d. difensivo del datore di lavoro sulle strutture informatiche aziendali in uso al lavoratore, a condizione che esso sia occasionato dalla necessità indifferibile di accertare lo stato dei fatti a fronte del sospetto di un comportamento illecito e che detto controllo prescinda dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa essendo, invece, diretto ad accertare la perpetrazione di eventuali comportamenti illeciti."*

35. Inoltre, la tesi della sopravvivenza dei "controlli difensivi", sotto il profilo della sua compatibilità con la tutela della riservatezza di cui all'art. 8 della Convenzione europea dei diritti dell'uomo, trova conforto nella giurisprudenza della Corte europea dei diritti dell'uomo che, in particolare nella sentenza di Grande Camera del 17 ottobre 2019, nel caso *Lòpez Ribalda e altri c. Spagna*. Si trattava di una fattispecie nella quale il gestore di un supermercato, dopo aver riscontrato discrepanze tra le scorte di magazzino e gli incassi di fine giornata, e sospettando che ciò dipendesse da illecite condotte appropriative di beni e/o denaro aziendale poste in essere da uno o più dipendenti, aveva installato all'interno del negozio dei dispositivi di videoripresa all'insaputa dei lavoratori, in posizione utile alla sorveglianza generalizzata ed indistinta di tutto il personale di volta in volta addetto al bancone di cassa, in tal modo appurando che le condotte sospettate si verificavano effettivamente. La Corte europea ha ritenuto la legittimità dell'iniziativa datoriale, in quanto proporzionata rispetto al fine (in sé legittimo) di tutelare l'interesse organizzativo-patrimoniale del datore di lavoro, ritenendo quindi che le corti nazionali avessero correttamente valutato che le misure adottate a tutela della *privacy* dei ricorrenti erano appropriate. La Corte europea ha osservato che : «(...) *se non è accettabile la posizione secondo cui anche il minimo sospetto di appropriazione illecita possa autorizzare l'installazione di strumenti occulti di videosorveglianza, tuttavia l'esistenza di un ragionevole sospetto circa la commissione di illeciti connotati da gravità e la prefigurazione dell'entità dei danni economici che possono derivarne, così come avvenuto nel caso concreto, possono costituire giustificazione legittimante di peso sufficiente grave.*[traduzione non ufficiale]»

36. Ciò, naturalmente, non vuol dire che il datore di lavoro, in presenza di un sospetto di attività illecita, possa avere mano libera nel porre in essere controlli sul lavoratore interessato.

37. Innanzitutto, va riaffermato il principio, già richiamato, espresso dalla giurisprudenza di questa Corte formatasi nel vigore della precedente formulazione dell'art. 4 dello Statuto dei lavoratori, secondo cui in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore (Cass. n. 15892 del 2007, cit.; Cass. n. 4375 del 2010, cit.; Cass. n. 16622 del 2012, cit.; Cass. n. 9904 del 2016; Cass. n. 18302 del 2016, cit.).

38. Occorrerà dunque, nel rispetto della normativa europea, e segnatamente dell'art. 8 della Convenzione europea dei diritti dell'uomo come interpretato dalla giurisprudenza della Corte europea dei diritti dell'uomo, assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, con un contemperamento che non può prescindere dalle circostanze del caso concreto (Cass. 26682/2017, cit.).

39. Non va infatti dimenticato che, nel caso *Barbulescu c. Romania*, sentenza della Grande Camera del 5 settembre 2017, la Corte europea dei diritti dell'uomo, chiamata a pronunciarsi – in relazione al detto articolo 8 - con riguardo ad una vidensa in cui un datore di lavoro aveva sottoposto a controllo il *software* aziendale *Yahoo Messenger* in uso al lavoratore, onde verificarne un indebito utilizzo, ha fornito una interpretazione estensiva del concetto di "vita privata", tanto da includervi la "vita professionale", così ritenendo che lo Stato rumeno avesse tenuto un comportamento non conforme alle garanzie accordate dalla norma della Convenzione, per avere le Corti nazionali omesso di accertare se il lavoratore avesse ricevuto una preventiva informazione dal suo datore di lavoro della possibilità che le sue comunicazioni su *Yahoo Messenger* potessero essere controllate; inoltre, per non avere valutato se il lavoratore medesimo fosse stato posto a conoscenza della natura e della estensione del controllo o del grado di intrusione nella vita e nella corrispondenza privata; infine, per non avere accertato le specifiche ragioni che giustificavano l'adozione di dette misure di controllo e se il datore di lavoro avrebbe potuto utilizzare misure meno intrusive, né se l'accesso al contenuto delle comunicazioni fosse stato compiuto senza che il lavoratore ne avesse consapevolezza.

40. Inoltre, e il punto è particolarmente rilevante nel caso in esame, per essere in ipotesi legittimo, il controllo "difensivo in senso stretto" dovrebbe quindi essere mirato, nonché attuato *ex post*, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto, sicché non avrebbe ad oggetto l'"attività" - in senso tecnico - del lavoratore medesimo. Il che è sostanzialmente in linea con gli ultimi approdi della giurisprudenza di questa Corte, più sopra richiamati, in materia di "controlli difensivi" nella vigenza della superata disciplina.
41. Occorre però chiarire cosa si intenda per tale controllo. Esso infatti non dovrebbe riferirsi all'esame ed all'analisi di informazioni acquisite in violazione delle prescrizioni di cui all'art. 4 St.lav., poiché, in tal modo opinando, l'area del controllo difensivo si estenderebbe a dismisura, con conseguente annientamento della valenza delle predette prescrizioni.
42. Il datore di lavoro, infatti, potrebbe, in difetto di autorizzazione e/o di adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché senza il rispetto della normativa sulla *privacy*, acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione, e, poi, invocare la natura mirata (*ex post*) del controllo incentrato sull'esame ed analisi di quei dati.
43. In tal caso, il controllo non sembra potersi ritenere effettuato *ex post*, poiché esso ha inizio con la raccolta delle informazioni; quella che viene effettuata *ex post* è solo una attività successiva di lettura ed analisi che non ha, a tal fine, una sua autonoma rilevanza.
44. Può, quindi, in buona sostanza, parlarsi di controllo *ex post* solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, *da quel momento*, alla raccolta delle informazioni.
45. Facendo il classico esempio dei dati di traffico contenuti nel *browser* del pc in uso al dipendente, potrà parlarsi di controllo *ex post* solo in relazione a quelli raccolti dopo l'insorgenza del sospetto di avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati.

Applicazione dei principi suesposti alla fattispecie in esame

46. Così ricostruito il quadro entro il quale i "controlli difensivi" tecnologici possono considerarsi ancora legittimi dopo la modifica dell'art. 4 dello Statuto dei

lavoratori, si deve rilevare che la sentenza impugnata, nel ritenere l'esorbitanza della fattispecie litigiosa dall'art. 4 dello Statuto dei lavoratori, ha osservato che il controllo sul *computer* aziendale in uso alla Ciamarra è stato indotto dalla necessità di verificare l'origine del *virus* che aveva infettato il sistema informatico della Fondazione criptando vari documenti e cartelle condivise, e di risolvere il problema; l'attività lavorativa, secondo la Corte di appello, è stata dunque sottoposta a verifica non durante il suo svolgimento, ma *ex post* e quale effetto indiretto di operazioni tecniche condotte su strumenti di lavoro appartenenti al datore di lavoro e finalizzate all'indifferibile ripristino del sistema informatico aziendale. In tale quadro, secondo la Corte territoriale, perderebbe quindi ogni importanza l'eccepita inutilizzabilità probatoria dei dati informatici acquisiti, inutilizzabilità ascritta dalla lavoratrice alla da lei allegata illecita acquisizione, presupposto da escludersi processualmente.

47. Se la statuizione della sentenza impugnata circa la serietà del sospetto di attività illecita indotto dalla scoperta del *virus* e dei danni da questo provocati può dirsi conforme alla necessità dell'accertamento del requisito del "fondato sospetto" della commissione di un illecito che i principi sopra ricostruiti assumono come presupposto della legittimità dei "controlli difensivi", è evidente come sia mancata ogni indagine nella stessa decisione volta a stabilire se i dati informatici rilevanti, utilizzati poi in sede disciplinare, fossero stati raccolti *prima* o *dopo* l'insorgere del fondato sospetto, in violazione dei principi esposti. È pure mancata ogni valutazione circa il corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore.

48. Come si è osservato, il controllo *ex post* non può riferirsi all'esame ed all'analisi di informazioni acquisite in violazione delle prescrizioni di cui all'art. 4 St.lav. *prima* dell'insorgere del "fondato sospetto", poiché, in tal modo opinando, l'area del controllo difensivo si estenderebbe a dismisura, con conseguente annientamento della valenza delle predette prescrizioni. Il datore di lavoro, infatti, potrebbe, in difetto di autorizzazione e/o di adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché senza il rispetto della normativa sulla *privacy*, acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione, e, poi, invocare la natura mirata (*ex post*) del controllo incentrato sull'esame ed analisi di quei dati.

49. Avendo ritenuto la fattispecie inquadrabile nei "controlli difensivi", ritenuti compatibili con la nuova formulazione dell'art. 4 Statuto dei lavoratori, la Corte territoriale non ha poi verificato la compatibilità del comportamento datoriale, e quindi della utilizzabilità dei dati informatici raccolti a fini disciplinari, con quest'ultima disposizione.

50. Il motivo in esame, anche se la Corte non ne condivide l'impostazione di fondo, volta ad escludere la sopravvivenza della legittimità dei "controlli difensivi" tecnologici, va dunque accolto per quanto di ragione, cioè in quanto esso evidenzia l'erroneità della statuizione della sentenza impugnata in ordine alla sussistenza dei presupposti della legittimità del "controllo difensivo" posto in essere dal datore di lavoro in assenza della verifica se esso avesse ad oggetto esclusivamente dati informatici raccolti successivamente all'insorgere del "fondato sospetto".

51. Il giudice di rinvio, da individuarsi nella stessa Corte di appello di Roma in diversa composizione, dovrà attenersi al seguente principio di diritto:

" Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto.

Non ricorrendo le condizioni suddette la verifica della utilizzabilità a fini disciplinari dei dati raccolti dal datore di lavoro andrà condotta alla stregua dell'art. 4 l. n. 300/1970, in particolare dei suoi commi 2 e 3."

52. I restanti motivi sono assorbiti, giacché essi presuppongono l'utilizzabilità dei dati litigiosi a fini disciplinari.

53. Segue alle svolte considerazioni l'accoglimento del primo motivo per quanto di ragione, con la cassazione della sentenza impugnata in relazione al motivo accolto, assorbiti gli altri, e con rinvio alla Corte di appello di Milano, in diversa composizione, che provvederà anche alle spese del presente giudizio di legittimità.

P.Q.M.

La Corte accoglie il ricorso in relazione al primo motivo, per quanto di ragione, assorbiti gli altri. Cassa la sentenza impugnata e rinvia alla Corte di appello di Roma, in diversa composizione, anche per le spese del giudizio di legittimità.

Così deciso in Roma, il 17 giugno e il 16 settembre 2021

Il Presidente est.

[redacted]

IL FUNZIONARIO GIUDIZIARIO
[redacted]
Depositato in Cancelleria
oggi, 22 SET. 2021
Il Funzionario Giudiziario

IL FUNZIONARIO GIUDIZIARIO
[redacted]