

Tribunale Roma, sez. lav., 24/03/2017

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO

Tribunale di Roma
SEZIONE LAVORO
Il Tribunale, nella persona del giudice designato Dott. ALFONSINA BELLINI Alla udienza del 24/03/2017 ha pronunciato la seguente

ORDINANZA

Fatto

Svolgimento del processo

Con ricorso ex art. 1, co. 48 legge n. 92/2012, ritualmente notificato, Ci. Pa. conveniva in giudizio la Fondazione Accademia Nazionale di Santa Cecilia chiedendo al giudice adito di accogliere le seguenti conclusioni:

Accertare e dichiarare l'illegittimità, la nullità e comunque l'inefficacia del licenziamento comminato alla dott.ssa Pa. Ci. con comunicazione del 29 gennaio 2016 e per l'effetto condannare la Fondazione Accademia Nazionale di Santa Cecilia alla reintegra della ricorrente nel posto di lavoro, con conseguente condanna dell'ente convenuto al pagamento in favore della ricorrente dell'indennità dell'ultima retribuzione globale di fatto pari ad E 3.744,89 mensili o altra, maggiore o minore, di giustizia, dalla data del licenziamento fino alla reintegra nel posto di lavoro, o altra data di giustizia e comunque nella misura massima di legge per i motivi di cui al ricorso.

in via subordinata :

Ritenuta comunque l'illegittimità, la nullità e comunque l'inefficacia del licenziamento comminato alla dott.ssa Pa. Ci. con comunicazione del 29 gennaio 2016, condannare la Fondazione Accademia Nazionale di Santa Cecilia al pagamento in favore della ricorrente dell'indennità di cui all'art. 18 legge 300/1970 nella misura massima o altra di giustizia dell'indennità pari all'ultima retribuzione globale di fatto pari ad € 3.744,89 o altra di giustizia oltre in ogni caso all'indennità sostitutiva del preavviso. Con vittoria di spese, i competenze ed onorari.

Espono la ricorrente di essere stata assunta nel 1987 ed inquadrata nel 2° livello ccnl Enti lirico sinfonici; di essere stata da ultimo adibita a decorrere dal 1 luglio 2008 all' Ufficio Contabilità alla Direzione Artistica quale addetta a funzioni di controllo del budget ed incaricata dell'assistenza logistica degli artisti ospitati, inquadrata da ultimo nel livello II del contratto aziendale sino alla data del licenziamento per giusta causa datato 29 gennaio 2016; che in ragione dell'attività espletata, era tenuta a utilizzare il PC e sistemi di navigazione internet e a inoltrare comunicazioni e informazioni a soggetti interni ed esterni all'ente; che il licenziamento era stato irrogato a seguito della contestazione disciplinare del 30 novembre 2015 nella quale addebitava alla ricorrente :

*Gentile Signora,
ai sensi e per gli effetti dell'art. 7 della L. n. 300/1970, abbiamo rilevato, e pertanto, Le contestiamo, quanto segue.*

In data 17 novembre u.s., alle ore 8:40 circa, una postazione informatica del sistema informativo della Fondazione ha contratto un virus, appartenente alla categoria dei cosiddetti virus "Crypto Locker", che colpisce generalmente attraverso l'apertura di link o allegati scaricati attraverso messaggi di posta elettronica e cripta tutti i dati del disco fisso, propagandosi poi sulla rete LAN.

Nel caso che qui interessa, il virus, oltre a criptare tutti i dati del disco della macchina infetta, ha iniziato a propagarsi sulla rete aziendale, criptando i file presenti all'interno dei dischi di rete denominati "Artistico", "Scambio", "Produzione" e "Rassegna Stampa".

I file progressivamente criptati dal virus sono risultati illeggibili e definitivamente inutilizzabili.

La prima attività svolta per proteggere il sistema ed evitare l'ulteriore propagazione del virus e, quindi, per arrestare il criptaggio dei file in condivisione, è stata quella di eliminare la condivisione dei dischi di rete.

Successivamente, per fermare il fenomeno, è stato necessario controllare tutti i client on line (circa 80) per individuare la postazione che aveva contratto il virus, ai fini della disattivazione della relativa scheda network.

Alle ore 13.00 circa dello stesso giorno è stato rinvenuta l'origine dell'infezione nel computer a Lei assegnato. Infatti, come risulta dai log e dai report allegati, il virus è stato contratto in conseguenza dell'apertura di un allegato scaricato, o di un link raggiunto, mediante account di posta privata.

Ai fini del ripristino della postazione è stato quindi necessario analizzare il disco locale della Sua workstation per risalire alle cause del contagio ed eliminare correttamente il virus.

In tale occasione, analizzando la cronologia di navigazione dell'unico browser utilizzato sul Suo computer (Google Chrome), nel periodo dal 16 ottobre al 16 novembre u.s. è risultato un numero abnorme di accessi a sistemi di posta elettronica privata (tramite webaccess e non attraverso applicativo dedicato) con una cadenza di pochi minuti l'uno dall'altro durante tutto l'orario lavorativo; sono altresì risultati numerosi accessi a siti di dubbia provenienza, (anch'essi vettori di malware, virus, trojan) tra i quali www.idealista.it, www.paginainizio.com, www.aforisticamente.com, www.frasionline.it, www.hoepli.it e www.immobiliare.it, come risulta dalla documentazione allegata alla presente lettera nella quale trova indicati in maniera analitica siti raggiunti, orari di navigazione e permanenza sui siti stessi. Detta documentazione, in ragione della voluminosità della stessa, viene allegata alla presente mediante incorporazione in un CD-Rom recante marca temporale e firma digitale. Gli indirizzi web cui si è connessa risultano, con pochissime eccezioni, del tutto estranei alle Sue incombenze di lavoro.

Le frequenze dei contatti dimostrano, inoltre, che le predette attività "ludiche", comunque del tutto estranee al rapporto di lavoro, hanno occupato, sempre nel periodo di riferimento, quasi l'intera durata della prestazione lavorativa giornaliera. Vi è da aggiungere che, ai fini del completo ripristino del sistema informativo aziendale, è stato necessario svolgere un'attività di disaster recovery che ha richiesto più giorni lavorativi, senza peraltro consentire il recupero completo di tutti i file danneggiati, alcuni dei quali risultano irrimediabilmente persi.

Tanto premesso, Le contestiamo, nel periodo dal 16 ottobre al 16 novembre 2015, l'impiego dei mezzi informatici messi a disposizione dal datore di lavoro per l'esecuzione della prestazione lavorativa a soli fini privati ed in violazione delle istruzioni impartite in ordine all'utilizzo degli stessi nonché dei più elementari doveri di diligenza, correttezza e buona fede nell'esecuzione della prestazione; aggiungiamo peraltro che, visti tempi e quantità di navigazione per fini privati, la Sua prestazione lavorativa è risultata sostanzialmente interrotta in tutto il periodo di riferimento.

Le contestiamo altresì di aver causato con il Suo operato gravi danni al patrimonio aziendale sia per la perdita dei dati che per l'impossibilità degli uffici di accedere alle cartelle danneggiate per tutto il tempo necessario al ripristino del sistema.

Le contestiamo altresì, per quanto occorra (vista l'estrema gravità degli addebiti sopra richiamati) anche la recidiva, tenuto conto del fatto che, a fronte di contestazione disciplinare datata 26 novembre 2013, prot.n. 10323, Le è stata applicata, in data 19 dicembre 2013, prot.n. 1539, la sanzione del licenziamento per giusta causa, successivamente convertita, per mera benevolenza ed in via transattiva, in sospensione dal servizio. Nel rilevare l'estrema gravità dei Suoi comportamenti, sia congiuntamente che disgiuntamente valutati, integranti violazione del vincolo fiduciario e dei più elementari doveri insiti nel rapporto di lavoro, Le ricordiamo che potrà fornirci le Sue eventuali giustificazioni entro 5 giorni dal ricevimento della presente contestazione.

La ricorrente presentava le sue giustificazioni negando di aver effettuato gli accessi contestati dalla parte convenuta.

La ricorrente eccepiva che le modalità con cui erano stati acquisiti i dati richiamati nella lettera di contestazioni erano invasive della privacy e lamentava che l'indicazione ed il trattamento dei siti indicati nella lettera di addebito risultavano effettuati in violazione delle disposizioni in materia di tutela della riservatezza, come accertato con il provvedimento dell'autorità garante sui dati personali del 1 marzo 2017 n. 13; che la ricorrente aveva, infatti, promosso ricorso al Garante per il trattamento dei dati personali al fine di ottenere il riconoscimento dell'illegittimo trattamento dei dati ed il conseguente blocco; che la parte convenuta aveva conservato i dati della cronologia di Google Chrome per un periodo di tempo ingiustificato e non aveva previsto un sistema di cancellazione automatico.

La ricorrente faceva rilevare che il trattamento e l'analisi dei siti aveva determinato l'acquisizione di informazioni personali in ordine a farmaci idonei a rivelare particolari patologie, ricerche su medici e strutture per cure specialistiche, ricerche su patologie specifiche.

Deduceva che l'ente convenuto non aveva comunicato alla ricorrente alcuna indicazione sulle modalità di trattamento dei dati della navigazione né sulle effettive caratteristiche del sistema né aveva acquisito alcun preventivo consenso al trattamento dei dati relativi.

Faceva rilevare che nella contestazione risultavano indicate asserite navigazioni notturne della ricorrente incompatibili con l'orario di lavoro, quale un sito asseritamente visitato alle 22:18 del

3.11.2015. Tanto premesso, faceva rilevare che la parte convenuta non aveva affisso in luogo accessibile alla dipendente il codice disciplinare.

Tanto premesso in fatto, eccepiva la nullità, illegittimità, invalidità e/o inefficacia del licenziamento deducendo che il fatto contestato non era stato posto in essere e che i risultati dell'illegittimo controllo al quale era stata sottoposta non potevano in nessun caso essere posti a fondamento del licenziamento.

Deducenza che il trattamento dei dati personali era avvenuto in assenza di autorizzazione e comunque in violazione delle informazioni e dei diritti rivendicati ai sensi dell'art. 7 dlgs 196/2003 per la cui violazione si riservava di rivendicare il danno non patrimoniale nelle sedi più opportune.

In ogni caso, in via subordinata, rilevava che la condotta contestata era inidonea a fondare il licenziamento per giusta causa alla luce della disciplina applicata in azienda e contestava l'assenza di un gravissimo danno patrimoniale per l'Accademia.

Contestava i presupposti della recidiva ex adverso invocata, deducendo che il precedente procedimento disciplinare, definito con accordo transattivo, era stato avviato con comunicazione del 26 novembre 2013, per cui il procedimento disciplinare del 30 novembre 2015 era stato posto in essere successivamente al biennio e, quindi, senza alcuna rilevanza.

Si costituiva in giudizio la convenuta contestando il ricorso di cui chiedeva il rigetto siccome infondato in fatto ed in diritto.

Deducenza che il codice disciplinare era affisso nelle bacheche di servizio poste in tre distinte ubicazioni: vicino all'ingresso del settore Uffici, in prossimità della sala S. Cecilia ed all'entrata della Sala Coro.

Specificava che a tutto il personale erano state rese note: le Regole di accesso al sistema informatico, gestione Personal Computer e disciplinare sull'utilizzo della posta aziendale; la procedura Trattamento e Protezione dei dati personali, la procedura Accessi fisici ai locali, le Regole di accesso alla Server farm dell'Auditorium Parco della Musica, procedura Custodia documenti cartacei e supporti Informatici.

Ampiamente argomentando in punto di diritto, insisteva nel rigetto della domanda.

Il giudice, escussi i testi citati, alla odierna udienza, all'esito del deposito di note autorizzate, si riservava.

Il ricorso è infondato.

L'Ente convenuto in data 30.11.2015 contestava alla ricorrente quanto segue:

... In data 17 novembre u.s. alle ore 8,40 circa, una postazione informatica del sistema informativo della Fondazione ha contratto un virus, appartenente alla categoria dei cosiddetti virus Crypto Locker, che colpisce generalmente attraverso l'apertura di link o allegati scaricati attraverso messaggi di posta elettronica e cripta tutti i dati del disco fisso propagandosi poi sulla rete LAN.

Nel caso che qui interessa, il virus, oltre a criptare tutti i dati del disco della macchina infetta, ha iniziato a propagarsi sulla rete aziendale, criptando i file presenti all'interno dei dischi di rete denominati Artistico, Scambio, Produzione e Rassegna Stampa.

I file progressivamente criptati dal virus sono risultati illeggibili e definitivamente inutilizzabili.

La prima attività svolta per proteggere il sistema ed evitare l'ulteriore propagazione del virus, è stata quella di eliminare la condivisione dei dischi di rete.

Successivamente, per fermare il fenomeno, è stato necessario controllare tutti i client on line (circa 80) per individuare la postazione che aveva contratto il virus, ai fini della disattivazione della relativa scheda network.

Alle ore 13 circa dello stesso giorno è stato rinvenuta l'origine dell'infezione nel computer a Lei assegnato. Infatti, come risulta dai log e dai report allegati, il virus è stato contratto in conseguenza dell'apertura di un allegato scaricato, o di un link raggiunto, mediante account di posta privata.

Ai fini del ripristino della postazione è stato quindi necessario analizzare il disco locale della Sua workstation per risalire alle cause del contagio ed eliminare direttamente il virus.

In tale occasione, analizzando la cronologia di navigazione dell'unico browser utilizzato sul Suo computer (Google Chrome), nel periodo dal 16 ottobre al 16 novembre u.s. è risultato un numero abnorme di accessi a

sistemi di posta elettronica provata tramite webaccess e non attraverso applicativo dedicato) con una cadenza di pochi minuti l' uno dall'altro durante tutto l'orario lavorativo; sono altresì risultati numerosi accessi a siti di dubbia provenienza ... come risulta dalla documentazione allegata ...

Gli indirizzi web cui si è connessa risultano, con pochissime eccezioni, del tutto estranei alla Sue incombenze di lavoro. Le frequenze dei contratti dimostrano, inoltre, che le predette attività "ludiche", comunque del tutto estranee al rapporto di lavoro, hanno occupato sempre nel periodo di riferimento quasi l'intera durata della prestazione lavorativa giornaliera. Vi è da aggiungere che, ai fini del completo ripristino del sistema informativo aziendale, è stato necessario svolgere un' attività di disaster recovery che ha richiesto più giorni lavorativi, senza peraltro consentire il recupero completo di tutti i file danneggiati, alcuni dei quali risultano irrimediabilmente persi.

Tanto premesso, Le contestiamo, nel periodo dal 16 ottobre al 16 novembre 2015, l'impiego dei mezzi informatici messi a disposizione dal datore di lavoro per l'esecuzione della prestazione lavorativa a soli fini privati ed in violazione delle istruzioni impartite in ordine all' utilizzo degli stessi nonché dei più elementari doveri di diligenza, correttezza e buona fede nell'esecuzione della prestazione; aggiungiamo peraltro che, visti tempi e quantità di navigazione per fini privati, la Sua prestazione lavorativa è risultata sostanzialmente interrotta in tutto il periodo di riferimento.

Le contestiamo altresì di aver causato con il Suo operato gravi danni al patrimonio aziendale sia per la perdita dei dati che per la impossibilità degli uffici di accedere alle cartelle danneggiate per tutto il tempo necessario al ripristino del sistema.

Le contestiamo altresì, per quanto occorra, (vista l'estrema gravità degli addebiti sopra richiamati) anche la recidiva, tenuto conto del fatto che, a fronte di contestazione disciplinare datata 26 novembre 2013 prot. N.10323 Le è stata applicata, in data 19 novembre 2013, prot. N. 1539, la sanzione del licenziamento per giusta causa, successivamente convertita, per mera benevolenza, ed in via transattiva, in sospensione dal servizio.

Nel rilevare l'estrema gravità dei Suoi comportamenti, sia congiuntamente che disgiuntamente valutati, integranti violazione del vincolo fiduciario e dei più elementari doveri insiti nel rapporto di lavoro, Le ricordiamo che potrà fornirci le Sue eventuali giustificazioni entro 5 giorni dal ricevimento della presente comunicazione.

A fronte di dette specifiche contestazioni, la ricorrente, nella lettera di giustificazioni deduceva :

Innanzitutto contesto integralmente e punto per punto il contenuto della Vostra contestazione, non avendo tenuto le condotte da Voi attribuitemi.

Dichiaro, inoltre, di aver sempre svolto il mio lavoro in modo diligente e puntuale, assolvendo con correttezza e precisione tutti i compiti che mi sono stati assegnati nel rispetto dei tempi e delle scadenze richieste.

In particolare, contesto integralmente la documentazione informatica da Voi consegnata a mezzo cd rom, la riferibilità degli accessi alla mia persona e l'intera procedura di acquisizione dei dati da Voi effettuata e la riferibilità dei dati alla mia persona ed al mio PC.

Evidenzio , a tal fine, che - sempre avendo a riferimento la Vostra contestata ricostruzione - risulterebbero dei miei accessi per uso personale in orari e giorni in cui non ero presente sul lavoro. In particolare, a titolo esemplificativo, il 3 novembre 2015, alle ore 22,18, quando in quella giornata ho cessato la mia attività lavorativa alle 14,19 ed il 5 novembre 2015 alle 18,43, quando in quella giornata ho cessato la mia attività lavorativa alle 14,20.

Rilevo in ogni caso di aver sempre rispettato le disposizioni aziendali in ordine all' utilizzo del sistema informatico. In tale prospettiva ho sempre seguito le indicazioni fornite dai tecnici informatici, lasciando che fossero loro a provvedere, come da precise indicazioni aziendali, al costante upgrade dei firewalls e del software antivirus, anche per tale motivo che la contestata infiltrazione, che si ribadisce non è a me in alcun modo addebitabile, non sarebbe, comunque, attribuibile ad una mia condotta lavorativa scorretta ...

La convenuta , nella memoria di costituzione, ha dedotto che, alle ore 13 del 17 novembre, l'origine della infezione era rinvenuta nel computer assegnato alla sig.ra Pa. Ci..

La convenuta ha altresì dedotto che nel corso della verifica, fu riscontrato - nel periodo immediatamente precedente (dal 16 ottobre al 16 novembre 2015) al verificarsi dell'infezione - un numero notevole di accessi durante l'orario lavorativo a sistemi di posta elettronica privata, tramite webaccess non attraverso applicativo dedicato, con cadenza di pochi minuti l'uno dall'altro; che si registrò una notevole quantità di

viste a siti internet di dubbia sicurezza e del tutto estranei alle incombenze di lavoro della ricorrente.

Dette circostanze possono ritenersi provate, pur tenuto conto della sommarietà del rito.

Infatti, il teste Di. Ba. ha dichiarato :

Io ho partecipato alle operazioni di verifica del sistema iniziate a novembre 2015. In quella occasione verificammo innanzitutto che il sistema informatico aveva contratto un virus; poi accertammo che il virus era del tipo Cripto locker . ADR. Analizzammo poi la fonte del virus per vedere da quale postazione era partito. ADR. Verificammo tutte le postazioni e accertammo che nessuna postazione , tranne una, aveva dei file criptati. ADR. Solo la postazione della ricorrente aveva dei files criptati. ADR. Tale tipologia di virus si innesca quando si scaricano file infetti dal web; per esempio attraverso la navigazione di siti poco sicuri oppure dal download di file anche attraverso posta elettronica o scaricati da internet. ADR. Nella cartella download del disco fisso era presente un file scaricato alle 8,40 che ha propagò il virus. Tale fu la prima analisi poiché dopo l' aver scaricato quel file, tutti i dati presenti sul server aziendali cambiarono estensione. ADR. Successivamente furono effettuati dei controlli sulla casella di posta elettronica della ricorrente per capire se vi era stato un invio di mail anomalo dall'esterno. Costatai che in quella mattinata ci furono della mail inviate dall'account di posta elettronica privato della ricorrente verso l'account di posta elettronica aziendale. Ho constatato che tale messaggio di posta elettronica venne classificato dal servizio antispam come SPAM. Non furono verificate le caselle di posta di tutto il personale poiché solo la postazione della ricorrente era infetta. ADR A quel punto la macchina della ricorrente è stata staccata dalla rete . ADR. Ribadisco che la causa del virus poteva essere solo quella che ho appena indicato. ADR Non ricordo se durante tali operazioni fosse presente la ricorrente; non ricordo se ero da solo nel momento in cui ho accertato quanto riferito; io ho condotto da solo la verifica.

Il teste Fa. Sa. ha dichiarato :

... Nel 2010 il Direttore del personale, coordinatore della privacy ha tenuto un corso di formazione, avente ad oggetto tutta la materia del Codice della Privacy nonché l'utilizzo dei sistemi informatici messa disposizione del datore di lavoro. A tale corso partecipò anche la ric. Dopo tale corso, è stata riformulata per tutto il personale la lettera di incarico al trattamento dei dati. Il corso era organizzato in sessioni che prevedevano la partecipazioni di gruppi di sei o sette persone. Preciso che il contenuto

del doc. 7 di parte convenuta è stato illustrato a tutto il personale durante il corso di cui ho prima riferito e all'esito è stato redatto un documento di sintesi che è stato collocato in una cartella di rete accessibile a tutti.

Parte ricorrente ha eccepito la inammissibilità ed irrilevanza delle disposizioni testimoniali, tenuto conto del fatto che, prima della introduzione del presente giudizio, la ricorrente aveva adito il Garante per la Protezione dei dati personali che, con provvedimento del 12.10.2016 che così provvedeva :
accoglie il ricorso e, per l'effetto, ordina alla resistente, ai sensi dell'art. 150, comma 2, del Codice, di astenersi, con effetto immediato dalla data di ricezione del presente provvedimento, dall'effettuare alcun ulteriore trattamento dei dati acquisiti secondo le modalità sopra descritte, eccettuata la mera conservazione degli stessi ai fini della loro eventuale acquisizione da parte giudiziaria;

Le eccezioni e contestazioni sollevate dalla difesa della ricorrente non appaiono condivisibili.

Osserva il codice di procedura civile non contiene alcuna norma che sancisce il principio di inutilizzabilità delle prove illegittimamente acquisite in violazione di legge.

Inoltre, l'art. 160 n. 6 dlgs 196/2003 stabilisce che la validità e l'utilizzabilità nel procedimento giudiziario di documenti, basati sul trattamento di dati personali non conforme a disposizioni di legge, restano disciplinate dalle pertinenti disposizioni processuali della materia penale e civile. Il contemperamento tra il diritto alla riservatezza e il diritto di difesa è rimesso, in assenza di una precisa norma processuale civile, alla valutazione del singolo giudice nel caso concreto (v. Tribunale Torino 8 maggio 2013 ,allegata dalla resistente.

Già la Suprema Corte (v. Cass. 5/8/2010 n. 18279) aveva avuto modo di affermare che, in tema di protezione dei dati personali, non costituisce violazione della relativa disciplina il loro utilizzo mediante lo svolgimento di attività processuale giacché detta disciplina non trova applicazione in via generale, ai sensi degli artt. 7, 24 e 46-47 del d.lgs. n. 193 del 2003 (cd. codice della privacy), quando i dati stessi vengano raccolti e gestiti nell'ambito di un processo; in esso, infatti, la titolarità del trattamento spetta all'autorità giudiziaria e in tal sede vanno composte le diverse esigenze, rispettivamente, di tutela della riservatezza e di corretta

esecuzione del processo, per cui, se non coincidenti, è il codice di rito a regolare le modalità di svolgimento in giudizio del diritto di difesa e dunque, con le sue forme, a prevalere in quanto contenente disposizioni speciali e, benché anteriori, non suscettibili di alcuna integrazione su quelle del predetto codice della privacy.

La Corte ha precisato che il contemperamento tra il diritto alla riservatezza e il diritto di difesa deve essere rimesso, in assenza di una precisa norma processuale civile, alla valutazione del singolo giudice nel caso concreto e ha chiarito che alle disposizioni che regolano il processo deve essere attribuita natura speciale rispetto a quelle contenute nel codice della privacy e nei confronti di esse, quindi, in caso di divergenza, devono prevalere (Cass. S. U. 8.2.1011 n. 3034).

Parte ricorrente si è opposta alla prova espletata richiamando quanto disposto nel Provvedimento n. 419 del 2016, reso dal garante della protezione dei dati personali.

Ebbene, proprio esaminando le conclusioni del provvedimento richiamato, risulta evidente che l'Autorità Amministrativa ha inteso salvaguardare la conservazione dei dati acquisiti dalla parte convenuta, ai fini dell'esercizio del proprio diritto di difesa in giudizio, nel momento in cui ha ordinato alla resistente di astenersi dall'effettuare alcun ulteriore trattamento dei dati acquisiti con le modalità accertate, eccettuata la mera conservazione degli stessi ai fini della loro acquisizione da parte giudiziaria.

Da ciò consegue che il diritto di difesa, a determinate condizioni, prevale rispetto al diritto alla riservatezza. Ed, infatti, l'art. 24 del Codice della Privacy prevede che il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento ... è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale.

Pertanto, deve concludersi che il Provvedimento n. 419 del 2016 non inibisce la conservazione e l'utilizzazione dei dati prodotti in giudizio;

diversamente argomentando, in quanto contenente limitazioni al diritto di difesa della parte convenuta, dovrebbe essere ritenuto illegittimo e, in quanto atto dell'autorità amministrativa, disapplicato dal giudice, ai sensi dell'art. 5 l. n. 2248 del 1865 ALL E.

A tale conclusione deve giungersi in ragione dei principi espressi dalla Suprema Corte nella sentenza n. 7341 del 2002 in cui viene affrontata la questione della natura giuridica delle autorità indipendenti, con specifico riferimento alla funzione svolta dal Garante per la privacy, in base all'art. 29 della legge 31.12.1996 n. 675.

La Corte, nella sentenza sopra richiamata ha così chiarito:
L'ordinamento anzitutto non conosce un *tertium genus* tra amministrazione e giurisdizione, alle quali la Costituzione riserva rispettivamente, per distinguerne e disciplinarne le attività, gli art 111 e 97.

Non vi è nel sistema costituzionale una figura di paragiurisdizionalità a se stante, distinta dalle due predette, ma piuttosto con l'uso di tale termine descrittivo si suole diffusamente indicare organi pubblici dotati di poteri la cui collocazione ha suscitato dubbi. Va altresì osservato che parte della dottrina nella immediatezza del sorgere nel paese del fenomeno delle Autorità Indipendenti, e la stessa sentenza impugnata, fondano la suddetta paragiurisdizionalità e sollevano i dubbi relativi al rapporto di siffatti soggetti pubblici con il giudice, sul connotato della terzietà. Nozione che solo di recente la Costituzione ha adottato in modo espresso nel testo novellato dell'art. 111, ma che da tempo è compresa nel lessico giuridico. Con essa si indica specificamente un carattere del giudice, che affianca quello ulteriore e diverso della imparzialità, costituito dal suo distacco, dal suo essere altro, rispetto agli interessi in conflitto. Si tratta dunque di stabilire se nel caso della Autorità in questione si possa parlare di terzietà, almeno nel senso che tale carattere basti a stabilire una natura assimilabile a quella giudiziaria e giustifichi la esclusione del soggetto pubblico così caratterizzato dal giudizio di impugnazione di un suo provvedimento. Ciò premesso va osservato che l'art. 102 della Costituzione stabilisce che la funzione giurisdizionale è esercitata da magistrati ordinari istituiti e regolati dalle norme sull'ordinamento giudiziario. Quindi al secondo comma vieta l'istituzione di giudici speciali e straordinari. È noto, provenendo dalla più accreditata dottrina cui il collegio aderisce, che non si istituisce un

giudice speciale solo con la attribuzione ad organo pubblico di un procedimento speciale.

È noto anche, ed il collegio condivide anche questa impostazione, che si considera giudice quel soggetto pubblico che esercitando quel tipico procedimento che è il processo giudiziario dà luogo ad una decisione su diritti suscettibile di assurgere alla definitività del giudicato, al di fuori di qualunque altro controllo da parte di altro e diverso organo o potere dello Stato. Non è dunque decisiva la considerazione dell'oggetto del decidere, giacché anche alle pubbliche amministrazioni è dato di provvedere su diritti in forme che la dottrina definisce giustiziali, e parimenti non è decisiva la considerazione dell'interesse pubblico costituente il riferimento fondamentale del giudice, perché in via di principio la P.A. provvede per l'appunto in considerazione di un interesse pubblico generale, la cui forza talvolta attenua la stessa protezione della posizione soggettiva, che degrada ad interesse legittimo.

Quanto alla struttura particolare del procedimento seguito dall'organo va osservato che a partire della legge n. 241 del 1990 l'ordinamento giuridico ha impresso alla attività della P.A. una svolta decisiva, attenuando progressivamente la storica caratterizzazione autoritativa del procedimento che sfocia in un provvedimento, per favorire il più ampio grado di partecipazione del soggetto interessato alla formazione del medesimo. Ciò talvolta a mezzo di un vero e proprio contraddittorio, analogo per forza di cose, a quello giudiziario che ne costituisce il modello, in coerenza con una lettura oramai dominante dell'art. 97 della Costituzione e dunque delle finalità di buon andamento e di imparzialità della amministrazione. È noto infatti, come afferma la migliore dottrina, che tra le funzioni del procedimento amministrativo vi è quella di far emergere con chiarezza il punto di contrasto tra il privato e la PA, cosicché anche il controllo giudiziario eventuale possa risultare perspicuo.

In tale ottica pertanto la diffusa tendenza alla introduzione nel procedimento amministrativo di momenti di partecipazione effettiva da parte degli interessati al suo esito che consentono alla PA di apprezzare tutti gli interessi in gioco, fa sì che l'uso di tali tecniche non significhi abbandono del procedimento in favore del processo. Ma piuttosto che l'obbligo di imparzialità, il quale richiede nella applicazione della legge la consapevolezza di tutte le posizioni tutelate, ancorché spettanti al

soggetto sottoposto alla autoritarità del provvedimento da emanare, viene realizzato anzitutto con l'articolazione del procedimento. In questo senso dire che la PA, ovvero una particolare P.A., è terza, vuol dire che essa ancorché provveda soddisfare l'interesse pubblico di cui è esponente, qualificando con gli effetti dell'atto amministrativo posizioni di parti anche contrapposte e da essa considerate in contraddittorio, fa uso del principio di imparzialità. Risulta pertanto decisivo, in adesione alla dominante dottrina, ad escludere la natura giurisdizionale, o paragiurisdizionale, se con tale termine si intende richiamare la predetta fonte giudiziaria del provvedimento, la sottoposizione della decisione dell'organo pubblico, comunque adottata, al vaglio di un giudice nei termini della domanda introduttiva del giudizio di controllo. Giacché essa fa desumere che il potere di attuare la legge a tali organi affidato non è comunque definitivo. 2d) Quanto alla Autorità in questione risulta altresì decisiva, e confermativa delle espresse conclusioni, la deduzione esegetica che si trae dall'art. 29, comma 7, della legge n. 675 del 1996, laddove si prevede che il Tribunale adito in opposizione alla delibera del Garante provvede "anche in deroga al divieto di cui all'art. 4 della legge n. 2248 del 1865, all. E". È infatti evidente che la deroga non avrebbe senso, nella mens legis, se non sul presupposto della natura amministrativa dell'organo e del suo procedimento, al quale la legge, proprio in considerazione della fragilità dei diritti della persona, toglie la protezione dalla intrusione del AGO nella attività amministrativa, altrimenti spettante.

Tanto premesso, quanto al rispetto dell'art. 4 l. n. 300/70, appare opportuna una rapida disamina del nuovo testo della norma.

Attraverso il D. Lgs. n. 151/2015, in vigore dal 24 settembre 2015, è stato riscritto l'art. 4 dello Statuto dei Lavoratori, modificando la disciplina in materia di strumenti informatici/tecnologici c.d. leggeri di universale dotazione dei dipendenti (smartphone, tablet, pc, ecc...) e di strumenti di controllo degli accessi e delle presenze (badge, tornelli di accesso a lettori magnetici, barre carraie con scheda rfid a distanza, ecc...).

Il nuovo primo comma dell'art. 4 dello Statuto dei Lavoratori identifica sempre nelle RSU e nelle RSA i soggetti con i quali devono essere stipulati gli accordi sindacali, prevedendo, in aggiunta rispetto alla

previgente disciplina, che nel caso di imprese con unità produttive ubicate in diverse province della stessa regione o in più regioni, l'accordo possa essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

La norma prosegue ribadendo, come in precedenza, che in caso di assenza del sindacato o di mancato accordo, si può procedere con autorizzazione da parte della Direzione Territoriale del Lavoro, ovvero, per le aziende con unità produttive ubicate in territori di competenza di diverse DTL, direttamente del Ministero del Lavoro.

Di fondamentale novità il nuovo comma 2 dell'art. 4 che riguarda gli strumenti informatico/tecnologici in dotazione al dipendente per svolgere l'attività lavorativa.

Per questi strumenti da oggi non trova più applicazione la procedura di autorizzazione e potranno essere utilizzati dai dipendenti (così come i badge e gli altri strumenti di accesso ai luoghi di lavoro) senza dover accedere ad un accordo sindacale o a preventiva autorizzazione amministrativa.

Presupposto per l'utilizzo a tutti i fini connessi al rapporto di lavoro dei dati raccolti da tali strumenti, precisa il comma 3 del nuovo art. 4, è che venga data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli e che sia rispettato quanto disposto dal D.Lgs. 30 giugno 2003, n. 196 (c.d. Codice Privacy).

I dati raccolti nel rispetto di quanto prescritto dalla norma possono, quindi, essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare.

Nella nuova formulazione dell'art. 4 dello Statuto dei Lavoratori (Legge 20 maggio 1970 n. 300), è solo apparentemente venuto meno il divieto esplicito di controlli a distanza, piuttosto la nuova formulazione ha adeguato l'impianto normativo alle innovazioni tecnologiche nel frattempo intervenute. Resta fermo, dunque, il divieto di controllare la sola prestazione lavorativa dei dipendenti, considerato che tale regime protezionistico è volto a tutelare la dignità e la riservatezza dei lavoratori, diritti la cui tutela è primaria nel nostro ordinamento, seppur da contemperare con le esigenze produttive ed organizzative o della sicurezza sul lavoro.

Il nuovo comma 1 dell'art. 4 elenca le ragioni giustificatrici che consentono al datore di lavoro – previo accordo collettivo aziendale (con RSA o RSU) - l'utilizzo di strumenti dai quali possa derivare, anche solo in via ipotetica, un controllo a distanza dei lavoratori:

- esigenze organizzative e produttive
- per la sicurezza del lavoro
- per la tutela del patrimonio aziendale

L'aspetto innovativo della norma, con riferimento alle esigenze giustificatrici dell'installazione e utilizzo di strumenti di controllo a distanza, è l'inserimento, tra i requisiti oggettivi, della tutela del patrimonio aziendale.

Tanto premesso, come correttamente fatto osservare dalla convenuta, lo strumento di lavoro, dovendo essere utilizzato ai fini della esecuzione della prestazione, può venire in rilievo ai fini dell'art. 4, comma 2, solo se il lavoratore ha un ruolo attivo nel suo utilizzo e, cioè, se quello strumento viene concretamente impiegato dal dipendente nello svolgimento delle mansioni.

Ciò che rileva è che lo strumento sia nella disponibilità del dipendente e da questi effettivamente utilizzato nell'adempimento della prestazione, diversamente da quanto avviene con gli strumenti di controllo di cui all'art. 4, comma 1, rispetto ai quali il lavoratore è invece, sempre soggetto passivo.

Pertanto, partendo dalla distinzione tra strumenti di lavoro e strumenti di controllo, l'uso degli strumenti informatici deve essere assimilato ad un mero strumento di lavoro messo a disposizione del lavoratore per rendere la prestazione; quindi i computer, i tablet ed i cellulari devono essere considerati come i moderni attrezzi di lavoro utilizzabili senza autorizzazione nel caso in cui vengano attribuiti al lavoratore per rendere la prestazione lavorativa oggetto del contratto di lavoro.

Orbene, nel caso in esame, considerate le mansioni svolte dalla ricorrente (impiegata amministrativa), il p.c. e la casella di posta elettronica non possono che essere considerati strumenti di lavoro necessari allo svolgimento della prestazione lavorativa; di conseguenza, devono ritenersi non necessari gli adempimenti di natura amministrativa e sindacale previsti dalla norma di cui all'art 4 cit.

Tanto premesso in fatto, osserva il giudice che l'art. 4 dello statuto dei lavoratori vieta le apparecchiature di controllo a distanza e subordina ad accordo con le r.s.a. o a specifiche disposizioni dell'Ispettorato del Lavoro l'installazione di quelle apparecchiature, rese necessarie da esigenze organizzative e produttive, da cui può derivare la possibilità di controllo.

La Suprema Corte ha affermato 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 (Cass., 17 giugno 2000, n. 8250), sul presupposto 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., n. 8250/2000, cit., principi poi ribaditi da Cass., 17 luglio 2007, n. 15892, e da Cass., 23 febbraio 2012, n. 2722).

Pertanto, il potere di controllo del datore di lavoro deve trovare un contemperamento nel diritto alla riservatezza del dipendente, ed anche l'esigenza, pur meritevole di tutela, del datore di lavoro 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.

Tale esigenza di tutela della riservatezza del lavoratore sussiste anche con riferimento ai cosiddetti "controlli difensivi" ossia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso, ove la sorveglianza venga attuata mediante strumenti che presentino quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro (Cass., n. 15892/2007, cit.; v. pure Cass., 1 ottobre 2012, n. 16622).

In tale ipotesi, è stato precisato, si tratta di " 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).

Diverso, però è il caso in cui il controllo sia diretto non già a verificare l'esatto adempimento delle obbligazioni direttamente scaturenti dal rapporto di lavoro, ma a tutelare beni del patrimonio aziendale ovvero ad impedire la perpetrazione di comportamenti illeciti; in tali casi , si è fuori dallo schema normativo della L. n. 300 del 1970, art. 4. 1.8.

In tali ipotesi, la Suprema Corte ha ritenuto che l'attività di controllo sulle strutture informatiche aziendali per conoscere il testo di messaggi di posta elettronica prescinde dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa ed è, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (Cass., n. 2722/2012).

E' stato inoltre precisato che le norme poste dalla L. 20 maggio 1970, n. 300, artt. 2 e 3, a tutela della libertà e dignità del lavoratore, delimitano la sfera di intervento di persone preposte dal datore di lavoro a difesa dei suoi interessi con specifiche attribuzioni nell'ambito dell'azienda (rispettivamente con poteri di polizia giudiziaria e di controllo della prestazione lavorativa), ma non escludono il potere dell'imprenditore, ai sensi degli artt. 2086 e 2104 c.c., di controllare direttamente o mediante la propria organizzazione gerarchica o anche attraverso personale esterno - costituito in ipotesi da dipendenti di una agenzia investigativa - l'adempimento delle prestazioni lavorative e quindi di accertare mancanze specifiche dei dipendenti già commesse o in corso di esecuzione, e ciò indipendentemente dalle modalità del controllo, che può avvenire anche occultamente, senza che vi ostino ne' il principio di correttezza e buona fede nell'esecuzione dei rapporti nè il divieto di cui alla stessa L. n. 300 del 1970, art. 4, riferito esclusivamente all'uso di apparecchiature per il controllo a distanza(Cass. 10 luglio 2009, n. 16196).

Nell'ambito dei controlli cosiddetti "occulti", la giurisprudenza della Suprema Corte ha avuto modo di affermarne la legittimità, ove gli illeciti del lavoratore non riguardino il mero inadempimento della prestazione lavorativa, ma incidano sul patrimonio aziendale (nella specie, mancata registrazione della vendita da parte dell'addetto alla cassa di un esercizio commerciale ed appropriazione delle somme incassate), e non presuppongono necessariamente illeciti già commessi

(Cass., 9 luglio 2008, n. 18821). In linea con questo stesso orientamento, si pone da ultimo, Cass., 4 marzo 2014, n. 4984, che ha ritenuto legittimo il controllo svolto attraverso un'agenzia investigativa, finalizzato all'accertamento dell'utilizzo improprio dei permessi ex L. n. 104 del 1992, ex art. 33, (suscettibile di rilevanza anche penale), non riguardando l'adempimento della prestazione lavorativa, in quanto effettuato al di fuori dell'orario di lavoro ed in fase di sospensione dell'obbligazione principale di rendere la prestazione lavorativa.

Da questo panorama giurisprudenziale, può trarsi il principio della tendenziale ammissibilità dei controlli difensivi "occulti", anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ferma comunque restando la necessaria esplicitazione 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 temperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale.

Ancor più recentemente, il Supremo Collegio ha precisato, in una fattispecie per certi versi, assimilabile a quella in esame, che il controllo eseguito dal datore di lavoro rispetta questi limiti e si pone al di fuori del campo di applicazione dell'art. 4 dello statuto dei lavoratori, quando non ha ad oggetto, in via diretta ed immediata, la prestazione lavorativa del dipendente. In particolare, la Corte ha affermato che il datore di lavoro ha posto in essere una attività di controllo che non ha avuto ad oggetto l'attività lavorativa più propriamente detta ed il suo esatto adempimento, ma l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente, poi effettivamente riscontrati, e già manifestatisi nei giorni precedenti, allorché il lavoratore era stato sorpreso al telefono lontano dalla pressa cui era addetto (che era così rimasta incustodita per oltre dieci minuti e si era bloccata), ed era stata scoperta la sua detenzione in azienda di un dispositivo elettronico utile per conversazioni via internet. Il controllo difensivo era dunque destinato a riscontare e sanzionare un comportamento idoneo a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti. Si è trattato di un controllo ex post, sollecitato dagli episodi occorsi nei giorni precedenti, e cioè dal riscontro

della violazione da parte del dipendente della disposizione aziendale che vieta l'uso del telefono cellulare e lo svolgimento di attività extralavorativa durante l'orario di servizio". (cfr. Cass. 27.5.2015 n. 10955).

Così definito l'ambito di applicazione dell'art. 4 , con riferimento al caso in esame, deve ritenersi legittimo il comportamento della parte convenuta. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa della ricorrente ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati). Più in particolare, il controllo c.d. difensivo è stato occasionato dalla necessità indifferibile di accertare lo stato dei fatti a fronte del sospetto di un comportamento illecito, con rilevanza penale.

La verifica su tutta la rete fu , infatti, avviata dalla Fondazione al solo scopo di contenere i danni al patrimonio aziendale e di verificare la sussistenza di un illecito anche di carattere penale da parte dei propri dipendenti.

Pertanto, come ha correttamente rilevato la convenuta nella memoria difensiva, la scoperta dell'abusivo utilizzo del computer aziendale non ha costituito il fine del controllo ma solo un esito accidentale di una verifica più ampia avente fini del tutto estranei al controllo sull'attività lavorativa.

Il c.d. controllo difensivo, in altre parole, non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la operatività dell'intero sistema informatico della convenuta. In questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio e la organizzazione del lavoro. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale. Orbene, quanto alla utilizzabilità dei dati, la norma dello statuto dei lavoratori consente che le informazioni raccolte possano essere utilizzate a condizione che sia data adeguata informazione al lavoratore in ordine alle modalità relative all'uso degli strumenti e alla esecuzione dei controlli, nel rispetto delle disposizioni contenute nel dlgs n. 196 del 2003.

Nel caso in esame, l' Accademia di Santa Cecilia ha prodotto in giudizio la Policy aziendale denominata Modello Organizzativo Primary, in cui sono analiticamente disciplinate le modalità relative sia all'uso degli strumenti che alla effettuazione dei controlli. E' infatti, espressamente previsto che l' Utente dei servizi è tenuto ad utilizzare solo ed esclusivamente per fini istituzionali dell' Accademia Santa Cecilia e non per scopi di lucro le applicazioni , le librerie di supporto, i documenti e quant' altro sia riferibile o faccia parte dei servizi fruiti; ogni altro uso deve essere preventivamente richiesto dall' utente ed autorizzato dal Responsabile del Servizio Informatico".

In tale disciplinare viene altresì specificato che Gli Utenti devono far uso dello Spazio Disco Utente nel pieno rispetto di quanto precedentemente enunciato. Per esigenze di servizio legate esclusivamente alla gestione delle Risorse Tecnologiche , gli Amministratori di Sistema potranno avere accesso allo Spazio Disco Utente.... Nel caso ciò avvenisse, gli Amministratori di Sistema provvederanno a mantenere riservate le informazioni, relative all' Utente, di cui potranno venire a conoscenza durante l'Accesso, fatta eccezione per quanto previsto e richiesto dalla legge.

Nel Disciplinare viene poi chiarito che Il servizio di posta elettronica è uno strumento di lavoro ed è offerto dalla Fondazione esclusivamente agli Utenti Abilitati come supporto per il raggiungimento di fini istituzionali o con lo scopo di inviare comunicazioni tecniche di servizio e/o informazioni su attività ed iniziative Dell' Accademia Nazionale di Santa Cecilia.

Si legge , poi, nello stesso documento, che la finalità è quella di evitare il rischio di utilizzo improprio del servizio di posta elettronica aziendale nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza.

Viene, inoltre, specificato che, proprio perché strumento di lavoro, sull'utilizzo sulla posta elettronica è ammesso un controllo della Fondazione

Infine, si specifica che l' uso della posta elettronica per esigenze personali è consentito, sempre nel rispetto di quanto sopra prescritto purchè tale utilizzo sia moderato, rispettoso dei limiti di congruità e della ragionevolezza. In nessun caso l'utente deve pregiudicare il normale funzionamento del servizio di posta elettronica aziendale".

La convenuta ha inoltre dedotto e provato, con i testi escussi, che le policy aziendali sono state rese pubbliche e i lavoratori, tra cui la ricorrente, hanno seguito una specifica formazione in materia di trattamento dei dati personali ex d.lgs 196/2003 e di utilizzo dei sistemi informatici.

Inoltre, i testi hanno confermato che la policy aziendale è stata sempre consultabile sulla rete aziendale della Accademia Santa Cecilia. Tale circostanza deve ritenersi in ogni caso confermata dalle stesse dichiarazioni rese dalla ricorrente, in sede di giustificazioni, allorquando ha affermato di aver sempre rispettato le disposizioni aziendali in ordine all' utilizzo del sistema informatico. Tali dichiarazioni evidenziano, infatti, in modo assolutamente inequivoco, che la convenuta aveva elaborato un sistema di norme disciplinanti il sistema informatico e che il personale ne era stato informato. Orbene, come dedotto dalla Fondazione e chiarito dai testi escussi, l' Accademia ha avuto accesso al personal computer della ricorrente, per mezzo dell'Amministratore del Sistema , solo dopo aver accertato la diffusione di un virus della rete aziendale e con la specifica finalità di bloccare la diffusione del virus e ripristinare il computer della ricorrente che era risultato infetto.

Dalle dichiarazioni dei testi escussi, come sopra riportate, è , quindi , emerso che , verificato che il sistema informatico aveva contratto un virus, venne poi accertato che il virus era del tipo crypto-locker; venne poi analizzata la fonte del virus per vedere da quale postazione era partito e, quindi, vennero controllate tutte le postazioni. All'esito di tale controllo, risultò che , nessuna postazione aveva dei file criptati tranne una. L'esame evidenziò che nella cartella download del disco fisso della ricorrente era presente un file scaricato alle 8,40 che aveva propagato il virus e , eseguiti controlli sulla casella di posta elettronica della ricorrente, risultò che vi era stato un invio di mail anomalo dall'esterno. Per tali ragioni, il computer della ricorrente venne staccato dalla rete.

Così ricostruiti i fatti, il licenziamento della ricorrente deve essere considerato legittimo.

In particolare, è risultato provato che la ricorrente ha abusato degli strumenti informatici a lei assegnati dal datore di lavoro, determinando un gravissimo danno all'intero sistema aziendale.

E' stato, infatti, dedotto e non specificamente contestato dalla ricorrente, che il virus, partito dal suo pc, oltre a criptare tutti i dati del disco della macchina infetta, iniziò a propagarsi nella rete aziendale, criptando i files presenti all'interno dei dischi di rete Artistico , Scambio e Rassegna Stampa. Inoltre, la convenuta ha dedotto, e sul punto non vi stata contestazione , che i files criptati risultarono illeggibili e inutilizzabili.

A fronte di tali specifici rilievi, la ricorrente, nella lettera di giustificazioni ha addotto solo generiche contestazioni.

Invero, nel ricorso introduttivo la ricorrente ha contestato espressamente di aver posto in essere il fatto materiale oggetto della contestazione contestandosi espressamente la realizzazione degli accessi oggetto della lettera di addebito".

Esaminando le dichiarazioni resi dai testi escussi, e tenuto conto di quanto sin qui dedotto, deve invece ritenersi provata la condotta imputata alla ricorrente e integrante la giusta causa di recesso. Il teste Ba. ha infatti chiarito che dall'esame della cartella di posta elettronica privata della ricorrente erano state inviate delle mail all'indirizzo di posta elettronica aziendale qualificati come SPAM. Il teste ha poi precisato che la tipologia di virus del tipo crypto-locker si innesca quando vengono scaricati file infetti dal web, per esempio, attraverso la navigazione di siti poco sicuri oppure dal download di file anche attraverso la posta elettronica o scaricati da internet.

Provato è, quindi, che la ricorrente abbia violato le istruzioni impartite in ordine all' utilizzo dei mezzi informatici messi a sua disposizione dal datore di lavoro per l'esecuzione della prestazione lavorativa; provato è, inoltre, che con tale condotta abbia arrecato danno al patrimonio aziendale certamente per l'impossibilità degli uffici di accedere alle cartelle danneggiate per tutto il tempo necessario al ripristino del sistema.

Inoltre, i tabulati in atti, non specificamente contestati dalla ricorrente, evidenziano il collegamento a siti che non avevano alcuna attinenza con la prestazione lavorativa, così provando il fatto che la prestazione era stata interrotta in tutto il periodo di riferimento.

Tale comportamento integra una giusta causa di recesso, atteso che gli addebiti mossi costituiscono un grave inadempimento, idoneo a ledere in maniera irreversibile il vincolo fiduciario, facendo venir meno l'affidamento del datore di lavoro nel futuro adempimento delle obbligazioni poste a carico del lavoratore.

Il ccnl applicato dalla convenuta prevede (v. art. 33) la sanzione del licenziamento "nei confronti del lavoratore colpevole di mancanze relative a doveri anche non particolarmente richiamati nel presente contratto che siano così gravi da non consentire la prosecuzione neanche provvisoria del rapporto di lavoro".

Quanto alla proporzionalità della sanzione, rileva il giudice che "In caso di licenziamento per giusta causa, ai fini della proporzionalità fra fatto addebitato e recesso, viene in considerazione ogni comportamento che, per la sua gravità, sia suscettibile di scuotere la fiducia del datore di lavoro e di far ritenere che la continuazione del rapporto si risolva in un pregiudizio per gli scopi aziendali, dovendosi ritenere determinante a tal fine, l'influenza che sul rapporto di lavoro sia in grado di esercitare il comportamento del lavoratore che denoti una scarsa inclinazione ad attuare diligentemente gli obblighi assunti, conformando il proprio comportamento ai canoni di buona fede e correttezza" (Cass. 7 luglio 2015 n. 13955).

Come si è sopra fatto rilevare, risulta provata la assenza di rispetto verso le procedure aziendali, sicchè il licenziamento deve ritenersi legittimo, trattandosi di condotta idonea a porre in dubbio la futura correttezza dell'adempimento in quanto sintomatica di un atteggiamento del lavoratore rispetto agli obblighi assunti.

Osserva il giudice che, ai fini della legittimità del licenziamento ciò che rileva sono le ripercussioni della condotta del lavoratore sul rapporto fiduciario senza che in senso contrario possano essere valorizzate circostanze quali la mancanza di precedenti disciplinari, la tenuità del danno e la mancanza di pregiudizio per l'azienda.

Né può richiamarsi la declaratoria contrattuale sul punto, atteso che la giusta causa di licenziamento è nozione legale e il giudice non è vincolato dalle previsioni del contratto collettivo.

In ordine alla eccepta mancata affissione del codice disciplinare, appare sufficiente rilevare che la garanzia, prevista dall'art. 7, primo comma, della Legge 20 maggio 1970, n. 300, di pubblicità del codice disciplinare mediante affissione in luogo accessibile a tutti, si applica al licenziamento disciplinare soltanto quando questo sia intimato per specifiche ipotesi di giusta causa o giustificato motivo previste dalla normativa collettiva o validamente poste dal datore di lavoro, e non anche quando faccia riferimento a situazioni giustificative del recesso previste direttamente dalla legge o manifestamente contrarie all'etica comune o concretanti violazione dei doveri fondamentali connessi al rapporto di lavoro (cfr. Cass. 3.10.2013 n. 22626).

Per tutte le considerazioni sin qui esposte, da ritenersi assorbenti di ogni altra eccezione, il ricorso deve essere respinto. Le spese seguono come per legge la soccombenza.

P.Q.M.

Respinge il ricorso e condanna la ricorrente al pagamento delle spese di lite che liquida in € 2.200,00, oltre iva e cpa.

Roma, 24 marzo 2017

Depositata in cancelleria il 24/03/2017.