REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO

CORTE DI APPELLO di ROMA

V Sezione Lavoro

La Corte composta dai signori magistrati:

dott.ssa Maria Antonia Garzia Presidente

dott. Carlo Chiriaco Consigliere

dott.ssa Alessandra Trementozzi Consigliere rel.

All'udienza del 17/11/2023 nella causa civile in grado di appello iscritta al n. 3872/2021 del Ruolo Generale degli affari contenziosi e vertente

tra

rappresentata e difesa dagli avv.ti Carlo de Marchis, Andrea Circi, Giacomo Summa, Filippo Aiello e Maria Matilde Bidetti, come da procura in atti,

ricorrente in riassunzione

e

in persona del legale rappresentante p.t., con gli avv.ti Domenico De Feo e Marco Marazza, che la rappresentano e difendono come da procura in atti

resistente in riassunzione

ha pronunziato la presente

SENTENZA

Oggetto: riassunzione a seguito della sentenza della Corte di Cassazione n. 25732/2021 del 22/09/2021

Conclusioni delle parti: come in atti

SVOLGIMENTO DEL PROCESSO

Con ricorso, depositato il 21.12.2021, ha riassunto il giudizio all'esito della pronuncia della Corte di Cassazione n. 25732/2021 del 22.9.2021, che ha cassato con rinvio la sentenza n. 1331/2019 di questa Corte

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

territoriale, chiedendo di "*Accertare e dichiarare la nullità, l'illegittimità e comunque l'inefficacia del licenziamento intimato alla ricorrente dalla in data 5 novembre 2015 e per l'effetto condannare la stessa alla reintegra nel posto di lavoro della dott.ssa in ogni caso, condannare la al pagamento in favore della dott.ssa della retribuzione/indennità e/o risarcimento pari alla retribuzione globale di fatto pari ad € 3.744,89 o alla maggiore o minore somma di giustizia dalla data del licenziamento all'effettiva reintegra o nella diversa misura di giustizia ovvero condannare la al pagamento dell'indennizzo, oltre al preavviso, nella misura massima di giustizia parametrata sulla retribuzione globale di fatto pari ad € 3.744,89 o altra di giustizia*", con in favore delle spese di lite per ogni fase e grado del giudizio da distrarsi.

La lite giudiziaria trae origine dal ricorso ex art. 1, co. 47 e ss., legge n. 92/2012 con cui la impugnava il licenziamento intimatole dalla data 29.1.2016, all'esito della contestazione disciplinare del 30.11.2015 con cui le veniva addebitato, nel periodo dal 16.10.1015 al 16.11.2015, l'utilizzo improprio del sistema informatico aziendale, che in tal modo veniva attaccato da un virus, il quale si propagava nel server provocando gravi danni alla Fondazione. In particolare veniva contestato alla lavoratrice sia l'utilizzo dei mezzi informatici aziendali per fini privati e per lo svolgimento di attività ludiche, che la sostanziale interruzione della prestazione lavorativa durante tali attività e il grave danno derivatone alla Fondazione a causa della perdita dei dati e comunque dell'impossibilità di accedere alle cartelle danneggiate per il tutto il tempo necessario al ripristino del sistema, nonché la recidiva con la precedente sanzione comminatale il 19.12.2013 (licenziamento disciplinare commutato in sede conciliativa in 60 giorni di sospensione dal servizio e dalla retribuzione).

La lavoratrice chiedeva di accertare l'illegittimità del licenziamento disciplinare e di condannare la Fondazione convenuta alla reintegrazione ai sensi dell'art. 18 legge 300/1970. In particolare la lavoratrice assumeva la propria estraneità ai fatti contestati, l'insussistenza della propria responsabilità e del danno addebitato e deduceva altresì l'illegittimità del controllo effettuato dalla datrice di lavoro sul PC in dotazione, assumendo illegittimo l'accesso alla cronologia browser di Google e alla posta elettronica per violazione dell'art. 4 dello Statuto dei lavoratori, nonché delle linee giuda dell'Autorità Garante per la

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

Protezione dei Dati Personali e della disciplina contenuta nel D.Lgs n. 196/2003, con conseguente inutilizzabilità a fini disciplinari dei relativi dati.

Giova evidenziare che, preventivamente all'impugnativa del licenziamento, la lavoratrice aveva presentato ricorso ex art. 145 del D.Lgs n. 196/2003 all'Autorità Garante per la Protezione dei Dati Personali che, con delibera del 12.10.2016, aveva ordinato alla Fondazione di astenersi dall'effettuare qualsiasi ulteriore trattamento dei dati acquisiti dalla cronologia del browser Google Chrome del computer in uso alla ricorrente per il periodo in contestazione "eccettuata la mera conservazione degli stessi ai fini della loro eventuale acquisizione da parte giudiziaria"; tale pronuncia veniva poi confermata dal Tribunale di Roma con sentenza n. 5987 del 28.03.2018, emessa a seguito del ricorso ex art. 152 del Codice in materia di protezione dei dati personali presentato dalla Fondazione.

Si costituiva in fase sommaria la Fondazione convenuta chiedendo il rigetto del ricorso per infondatezza dello stesso, sussistendo la legittimità del licenziamento per giusta causa e chiedendo in subordine la riqualificazione in giustificato motivo soggettivo. In particolare, assumeva il carattere "difensivo" del controllo operato sul computer in uso alla lavoratrice.

Escussi i testi, con ordinanza del 24.3.2017 il giudice della fase sommaria rigettava il ricorso, ritenendo dimostrati i fatti addebitati, con conseguente sussistenza della giusta causa di licenziamento, dovendosi ritenere l'inadempimento di gravità tale da non consentire la prosecuzione del rapporto.

Avverso tale ordinanza proponeva opposizione

Radicatosi il contraddittorio, il giudice dell'opposizione rilevava che la delibera dell'Autorità Garante del 12.10.2016 non ostava alla utilizzazione nel processo dei dati estratti dal computer aziendale in uso alla lavoratrice, tanto più che secondo tale delibera i dati in questione erano conservabili dalla parte datoriale a fini della difesa in giudizio. Osservava il Tribunale che l'acquisizione dei predetti dati non si era risolta in un controllo a distanza in violazione dell'art. 4, legge n. 300/1970, essendo stata la verifica del datore di lavoro finalizzata a bonificare il sistema informatico della Fondazione da un virus e non dall'intento di verificare l'esecuzione della prestazione lavorativa dovuta dalla

. Considerato che il comportamento della lavoratrice non aveva determinato il rischio dell'applicazione di una sanzione prevista dal D.Lgs. n.

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

231/2001 nei confronti della Fondazione e che non appariva del tutto incompatibile con le mansioni della lavoratrice, non essendo stata contestata la mancata esecuzione di specifiche incombenze lavorative, non lo considerava idoneo a ledere irreparabilmente il rapporto di fiducia con l'ente. Pertanto, rilevava la sproporzione della sanzione espulsiva e condannava la Fondazione alla reintegrazione ai sensi dell'art. 18 della legge n. 300/1970, nel testo applicabile al pubblico impiego privatizzato.

Pronunciandosi sul reclamo proposto dalla Fondazione e su quello incidentale della , questa Corte territoriale, in riforma della sentenza del Tribunale, rigettava il ricorso introduttivo proposto dalla condannandola al pagamento delle spese di entrambi i gradi del giudizio.

In particolare questa Corte condivideva le argomentazioni del Tribunale secondo cui i dati acquisiti dal computer aziendale in uso alla relativi al periodo 16 ottobre – 16 novembre 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. Escludeva inoltre la dedotta violazione dell'art. 4 dello Statuto dei lavoratori atteso che, come già accertato dal Tribunale, il controllo sul computer aziendale della si era reso necessario per verificare l'origine del virus che aveva infettato il sistema informatico della Fondazione, criptando dati e causandone in parte la perdita irrimediabile. Condivisa la ricostruzione dei fatti operata dal Tribunale, questa Corte però rilevava: - che l'ingente numero di accessi ad internet aveva natura ludica e privata; - 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); - che dai numerosi accessi ad internet per fini personali era risultata frammentata la prestazione lavorativa, resa in maniera discontinua. Pertanto, evidenziata l'intenzionalità della condotta, riteneva proporzionata la sanzione espulsiva per violazione dell'art. 33 del CCNL applicato dall'ente, avendo la lavoratrice consapevolmente trasgredito alle indicazioni datoriali sull'utilizzo degli strumenti informatici, indicazioni delle quali era stata compiutamente resa edotta, così sottraendo energie alla prestazione lavorativa ed incrinando irrimediabilmente la fiducia sulla correttezza del futuro adempimento della prestazione, tenuto conto anche della sanzione disciplinare già irrogatale nel 2013 per un addebito

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

analogo a quello oggetto di contestazione.

Avverso tale sentenza ha proposto tempestivo ricorso in Cassazione

censurando la sentenza di questa Corte territoriale per i seguenti motivi:

1. violazione e falsa applicazione dell'art. 2119 c.c., dell'art. 4 della legge 20 maggio 1970 n. 300, dell'art. 160 comma 6 del Codice della privacy, dell'art. 2702 e ss. c.c. e degli artt. 115 e 245 c.p.c. 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;
2. violazione e falsa applicazione dell'art. 2119 c.c., dell'art. 18 comma 4 legge 20 maggio 1970 n. 300 nonché degli artt. 1362, 1363, 1364 e 1365 c.c. e dell'art. 1370 c.c. in relazione alle disposizioni del codice etico e del sistema disciplinare dell' 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 posti dall'art.4 dello Statuto dei lavoratori, la Corte di merito non avrebbe potuto distaccarsi dalla tipizzazione degli illeciti contenuta nel codice etico e nel sistema disciplinare;
3. violazione dell'art. 112 c.p.c., degli artt. 1362, 1363, 1364 e 1365 c.c. e dell'art. 347 c.p.c. con riferimento alla eccezione di tardività della precedente sanzione della sospensione di 10 giorni, irrogata alla Ciamarra in esito ad un accordo intervenuto tra le parti in occasione del pregresso procedimento disciplinare ed omessa pronuncia sull'eccezione di inutilizzabilità ai fini della recidiva della stessa.

Si costituiva la Fondazione resistendo con controricorso.

Con sentenza n. 25732/2021 la Suprema Corte, ricostruito il sistema normativo prima e dopo la nuova formulazione dell'art. 4 della legge 300/1970 introdotta dall'art. 23 del D.Lgs 151/2015, ha censurato la sentenza di questa Corte territoriale nella parte in cui *"… 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 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*

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

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" (così pag. 19 della sentenza rescindente).

Ritenuti assorbiti gli ulteriori due motivi di gravame, la S.C. ha pertanto cassato la sentenza con rinvio a questa Corte, formulando il 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

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

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".

ha dunque riassunto il giudizio deducendo l'illegittimità ed invasività del controllo ex post effettuato sul proprio account, con conseguente inutilizzabilità dei dati acquisiti. Ha inoltre riproposto le censure ritenute assorbite dalla S.C. in merito alla sproporzione della sanzione espulsiva con riferimento alle previsioni del codice disciplinare, state l'insussistenza di alcun concreto danno alla Fondazione e la natura colposa dell'infrazione.

Si è costituita la Fondazione resistendo al ricorso in riassunzione e chiedendo il rigetto di tutte le domande avanzate dalla . In particolare ha evidenziato come il principio di diritto formulato dalla S.C. demanda a questa Corte di verificare la riconducibilità delle verifiche effettuate ai controlli difensivi così come ricostruiti nell'esercizio della sua funzione nomofilattica, ma precisa che, non ricorrendone le condizioni, la verifica dell'utilizzabilità a fini disciplinari dei dati raccolti andrà effettuata ai sensi dei commi 2 e 3 dell'art. 4 della legge 300/1970. Secondo la resistente in riassunzione, nel caso in esame sussisterebbero tutti i requisiti di cui al comma 2 della citata disposizione, essendo stata fornita alla lavoratrice una adeguata informativa, come emerso dalle prove documentali e testimoniali acquisite in fase sommaria. Ritenuta la non vincolatività del provvedimento del garante, la Fondazione resistente ha ribadito la proporzionalità della sanzione espulsiva e la legittimità della contestata recidiva. Ha dunque rassegnato le seguenti conclusioni: "*a) rigettare le domande tutte di cui al ricorso ex art. 1, commi 47 e segg. L. n. 92/2012 proposto dalla sig.ra - reiterate nel ricorso ex art. 392 c.p.c. - in quanto del tutto infondate in fatto ed in diritto, dichiarando per l'effetto la legittimità del licenziamento per giusta causa irrogato alla lavoratrice, anche previa eventuale riqualificazione dello stesso come recesso per giustificato motivo soggettivo; b) in subordine, nella denegata ipotesi di applicazione dell'art. 18, comma 5, L. n. 300/70, dichiarare risolto il rapporto di lavoro, condannando la Fondazione al pagamento di una indennità risarcitoria nella misura minima di legge, o nella diversa misura ritenuta di giustizia; c) in ulteriore subordine, nella denegata ipotesi di applicazione dell'art. 18, comma 4, L. n. 300/70, condannare la Fondazione al pagamento di una indennità risarcitoria nella misura minima o nella diversa misura ritenuta di giustizia; d) in ogni caso detrarre dalle somme eventualmente dovute i redditi da lavoro percepiti aliunde e quelli percipiendi usando*

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

l'ordinaria diligenza; e) condannare la sig.ra al pagamento delle spese di causa".

All'udienza del 8.9.2023 la causa è stata trattenuta in decisione nelle forme di cui alla legge 92/2012.

MOTIVI DELLA DECISIONE

Dovendo pronunciarsi nei limiti del devoluto, sulla base dei principi di diritto sanciti dalla sentenza rescindente, osserva questo Collegio che la S.C. ha rimesso la causa a questo Collegio per la verifica della sussistenza di un fondato sospetto preesistente all'acquisizione dei dati informatici comprovanti la commissione di un illecito. Dunque, a questa Corte è demandato di verificare se i dati informatici siano stati raccolti prima o dopo l'insorgere del fondato sospetto di commissione da parte della lavoratrice di fatti illeciti e se l'acquisizione degli stessi sia avvenuta rispettando il corretto bilanciamento fra le esigenze aziendali e la tutela della dignità e della riservatezza della lavoratrice. Solo in caso in cui i dati non fossero stati acquisiti dopo l'insorgere del fondato sospetto e in carenza del suddetto bilanciamento, questo Collegio dovrà verificare l'utilizzabilità degli stessi ai sensi dei commi 2 e 3 dell'art. 4 dello Statuto dei lavoratori.

Nella memoria difensiva in sede di opposizione la Fondazione resistente ribadiva che:

- in data 17.11.2015, alle ore 8,40, una delle postazioni informatiche della Fondazione era stata colpita da un virus informatico che, oltre a criptare tutti i dati del PC, si era propagato nella rete aziendale, criptando i files contenuti nei dischi di rete denominati "Artistico", "Scambio", "Produzione" e "Rassegna Stampa";
- alle ore 13 dello stesso giorno l'origine dell'infezione veniva individuata nel computer in uso alla , in conseguenza dell'apertura di un allegato scaricato o di un link raggiunto attraverso l'account di posta privata della lavoratrice;
- per risalire alle cause del contagio ed eliminare il virus era stato necessario analizzare il disco locale del PC assegnato alla
- nel corso di tale verifica fu riscontrato che nel periodo immediatamente precedente (dal 16 ottobre al 16 novembre 2015) al verificarsi dell'infezione un notevole numero di accessi effettuati durante l'orario lavorativo all'account di posta elettronica privata tramite webaccess;

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

- inoltre nello stesso periodo veniva riscontrato una notevole quantità di navigazioni su siti internet di dubbia sicurezza effettuate durante l'orario lavorativo.

Il teste , escusso in fase sommaria ha dichiarato: "In quella occasione verificammo innanzitutto che il sistema informatico aveva contratto un virus; poi accertammo che il virus era del tipo Crypto Locker. Analizzammo poi la fonte del virus per vedere da quale postazione era partito. Verificammo tutte le postazioni e accertammo che nessuna postazione, tranne una, aveva dei file criptati. Solo la postazione della ricorrente aveva dei files criptati. Tale tipologia di virus si innesca quando si scaricano file infetti da web; per esempio attraverso la navigazione di siti poco sicuri oppure dal download di file anche attraverso posta elettronica o scaricati da internet. Nella casella download del disco fisso era presente un file scaricato alle 8,40 che propagò il virus. Tale fu la prima analisi poiché dopo l'aver scaricato quel file, tutti i dati presenti sul server aziendali cambiarono estensione. 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. Constatai che in quella mattinata ci furono delle mail inviate dall'account di posta elettronica privato della ricorrente verso l'account di posta 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. A quel punto la macchina della ricorrente è stata staccata dalla rete. Ribadisco che la causa del virus poteva essere solo quella che ho appena indicato. (…) Io ho condotto da solo la verifica".

Dunque, in relazione all'accertamento demandato a questo Collegio dalla S.C., emerge che la acquisizione dei dati informatici utilizzati in sede disciplinare è stata effettuata prima dell'insorgere del fondato sospetto dell'espletamento di attività illecite da parte della lavoratrice, atteso che proprio dai dati raccolti sono emerse le condotte oggetto di contestazione. Invero, come statuito dalla S.C. "*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. 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*

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati" (così i punti 44 e 45 della sentenza rescindente).

E' indubbio che, come ribadito dalla recente sentenza della S.C. n. 18168/2023, "*incomba sul datore di lavoro l'onere di allegare prima e provare poi le specifiche circostanze che lo hanno indotto ad attivare il controllo tecnologico ex post, considerato che solo tale "fondato sospetto" consente al datore di lavoro di porre la sua azione al di fuori del perimetro di applicazione diretta dell'art. 4 St. lav. e tenuto altresì conto del più generale criterio legale ex art. 5 l. n. 604 del 1966 che grava la parte datoriale dell'onere di provare il complesso degli elementi che giustificano il licenziamento*".

Nel caso in esame resistente non ha mai dedotto la sussistenza di concreti e riconoscibili indizi della commissione di comportamenti illeciti da parte della lavoratrice prima dell'acquisizione dei dati contenuti nel computer alla stessa assegnato.

Pertanto, in applicazione del principio di diritto sancito dalla S.C., deve escludersi che l'acquisizione dei dati informatici sul computer assegnato alla rientri nei controlli difensivi.

La sentenza rescindente ha quindi demandato a questa Corte di verificare l'utilizzabilità dei dati raccolti in applicazione dei commi 2 e 3 dell'art. 4 della legge n. 300/1970. Tali commi prevedono l'inapplicabilità delle disposizioni previste al comma 1 del medesimo art. 4 agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e a quelli per la registrazione delle presenze e stabiliscono che le informazioni raccolte in base ai 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" (così il comma 3).

Dunque, l'utilizzabilità dei dati raccolti sugli strumenti utilizzati dal lavoratore per svolgere la prestazione lavorativa, fra cui il computer assegnato alla ricorrente, è subordinata alla circostanza che il lavoratore abbia ricevuto adeguata informazione non solo delle modalità di uso degli strumenti, ma anche dell'effettuazione dei controlli e che sia stato rispettato il disposto del D.Lgs n. 196/2003.

Quanto all'informazione preventiva, il teste ha dichiarato che: "Nel 2010 il Direttore del personale, coordinatore della privacy, ha tenuto un corso di formazione, avente ad oggetto tutta la materia del Codice della

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

Privacy nonché l'utilizzo dei sistemi informatici messi a disposizione del datore di lavoro. A tale corso partecipò anche la ricorrente. 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 partecipazione 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". Proprio il doc. 7 allegato al fascicolo della fase sommaria dell'odierna resistente contiene le Regole d'accesso al sistema informativo e di gestione del personal computer, disponendo che "Per esigenze di servizio legate esclusivamente alla gestione delle risorse tecnologiche, gli amministratori di sistema potranno avere accesso allo spazio disco utente (operazione chiamata qui di seguito accesso). 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". Quanto all'utilizzo del servizio di posta aziendale, il regolamento prevede che in caso di anomalie "possono essere effettuate delle verifiche effettuate su dati aggregati riferiti all'intera struttura ovvero su singole aree". Il disciplinare in esame consente altresì l'utilizzo per esigenze personali dell'account di posta aziendale "… purché tale utilizzo sia moderato, rispettoso dei limiti di congruità e della ragionevolezza". Inoltre, il regolamento espressamente dispone che "Per esigenze legate esclusivamente alla gestione del servizio di posta elettronica (ad esempio in caso di disservizi nel funzionamento dei server di posta), gli amministratori di sistema possono accedere ai log di sistema relativi agli indirizzi e-mail. (…) Le caratteristiche relative alla procedura di accesso e conservazione dei log di sistema sono indicate nella procedura "Conservazione Log". L'Accademia effettua settimanalmente il backup del fileserver e degli archivi di posta elettronica ed a giorni alterni delle copie incrementali/differenziali dei dati su unità storage dedicati …". Il Tribunale di Roma, con la sentenza n. 5987/2018 del 28.3.2018, resa in sede di opposizione della Fondazione al provvedimento del Garante per la protezione dei dati personali ha rilevato che *"… pur potendosi prescindere dalla questione relativa alla conoscenza da parte della del disciplinare e della relativa informativa collettivamente resa dal datore di lavoro riguardo ad esso, non avendo mai la*

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

resistente, nemmeno innanzi al Garante, dedotto di non averne avuto notizia (del resto la stessa risulta nominata in data 13.7.2010, come da documentazione allegata, "incaricata del trattamento di dati personali"), tale Modello Organizzativo Privacy (nella parte specificamente denominata "Regole d'accesso al Sistema Informativo, gestione Personal Computer e disciplinare sull'utilizzo della posta aziendale") non risulta affatto conforme alle linee guida del Garante del 2007, specie per quel che concerne la navigazione in Internet da parte del dipendente, punto sul quale peraltro si incentrano gli addebiti nei suoi confronti e le più consistenti violazioni della riservatezza da parte del datore di lavoro.

Il disciplinare in questione – mentre dispone di una specifica parte relativa all'utilizzo del servizio di posta aziendale (che comunque consente espressamente l'uso della posta elettronica aziendale per esigenze personali purchè "tale utilizzo sia moderato, rispettoso dei limiti di congruità e della ragionevolezza") - è infatti assolutamente carente sull'argomento Internet, nulla essendo previsto al riguardo di quanto menzionato nelle linee guida, nemmeno con riferimento a quanto in esse indicato circa l'adozione di misure opportune a prevenire l'utilizzo improprio di Internet e la conservazione dei dati personali relativi agli accessi ad Internet effettuati dai dipendenti (previsioni nel disciplinare esistenti solo relativamente al server di posta elettronica).

La fondazione ricorrente quindi, tramite l'attività di controllo svolta in conseguenza dell'anomalia risultata nella casella di posta elettronica della dipendente, ha avuto accesso indebitamente alla cronologia di siti internet da essa visitati nel corso di un intero mese, alcuni dei quali idonei anche a rivelare dati sensibili della medesima, quali in particolare condizioni di salute (cfr., schermate allegate in atti).

Del resto, alla pubblicizzazione del predetto disciplinare deve affiancarsi, per come previsto dalle stesse linee guida ("rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli"), l'obbligo del datore di lavoro di informativa ex art. 13 del Codice Privacy, nella specie non avvenuto". La accertata violazione degli obblighi di comunicazione preventiva di cui all'art. 13 del codice della privacy all'epoca vigente (adesso art. 13 del Regolamento europeo) preclude l'utilizzabilità dei dati raccolti a fini disciplinari. Infatti, come condivisibilmente osservato dal Tribunale di Roma nella sentenza sopra richiamata, il disciplinare conteneva specifiche previsioni sul trattamento e sulla conservazione dei dati personali solo relativamente al server di posta elettronica aziendale. Difettano invece nel regolamento in esame, che la Fondazione resistente ha integralmente trascritto nella memoria difensiva in riassunzione, regole sulla conservazione dei dati

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

personali relativi alle navigazioni Internet effettuate dai dipendenti. Invero, sebbene nel regolamento sopra richiamato sia espressamente vietato l'utilizzo dei servizi informatici per fini diversi da quelli istituzionali e venga prevista la possibilità di accesso al disco utente, non vengono in alcun modo regolamentate le modalità di conservazione e trattamento dei dati risultanti dalla cronologia browser della navigazione su internet.

Ne consegue che i dati relativi agli accessi della alla cronologia delle navigazioni su internet (quindi compresi quelli relativi all'accesso alla casella di posta elettronica privata), sono inutilizzabili a fini disciplinari.

L'inutilizzabilità a fini disciplinari dei dati posti a fondamento della contestazione disciplinare per carenza di una adeguata informativa sulla conservazione degli stessi, determina l'insussistenza dei fatti contestati.

Deve pertanto essere dichiarata l'illegittimità del licenziamento intimato alla in data 29.1.2016, con conseguente condanna della Fondazione alla immediata reintegrazione della lavoratrice nel posto di lavoro precedentemente occupato e al pagamento delle retribuzioni globali di fatto maturate dal licenziamento sino all'effettiva reintegra, oltre interessi e rivalutazione monetaria come per legge, nonché alla regolarizzazione della posizione contributiva e previdenziale.

Restano assorbite le altre questioni devolute al grado.

Le spese seguono la soccombenza come per legge e si liquidano nella misura di cui in dispositivo, così determinata in applicazione dei criteri previsti dal D.M. 55/2014 e successive modificazioni ed integrazioni, con attribuzione ai procuratori antistatari.

P.Q.M.

La Corte, pronunciando nei limiti del devoluto, così provvede:

dichiara illegittimo il licenziamento intimato a in data 29.1.2016;

condanna la Fondazione resistente all'immediata reintegrazione della lavoratrice nel posto di lavoro precedentemente occupato ed al pagamento delle retribuzioni globali di fatto maturate dal licenziamento all'effettiva reintegra, oltre accessori, nonché alla regolarizzazione della sua posizione contributiva e previdenziale;

condanna la Fondazione resistente al pagamento delle spese processuali che liquida quanto alle fasi del primo grado in complessivi € 6.000,00, quanto

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad

all'appello in € 4.500,00, quanto al giudizio di Cassazione in € 3.200,00 e quanto al presente giudizio in € 4.250,00, oltre rimborso spese forfettario in misura pari al 15%, IVA e CPA come per legge, da distrarsi.

Così deciso in Roma, il 17/11/2023

Il Consigliere estensore
Dott.ssa Alessandra Trementozzi

La Presidente
dott.ssa Maria Antonia Garzia

Firmato Da: GARZIA MARIA ANTONIA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 106cc626eb9ecafa994e6531d0d66fa9
Firmato Da: TREMENTOZZI ALESSANDRA Emesso Da: ARUBAPEC PER CA DI FIRMA QUALIFICATA Serial#: 4085fd967f778f268d1025850f54bdad