TRIBUNALE DI NAPOLI
SEZIONE LAVORO
ORDINANZA
(art. 1 c. 47 L 92/2012)

IL GL, dr. ssa Antonella Ciriello

sciogliendo la riserva posta all'udienza del 4.12.2013, nel giudizio sommario ex art. . 1 commi 47 e ss. L 92/2012 , R.G. 35065 /2012 tra

P[redacted] M[redacted], rappresentata e difesa in virtù di procura a margine del ricorso, dall'avv. RIZZO GAETANO nonché dall'avv. presso cui elettivamente domicilia giusta procura in atti in VIA S. LUCIA 97 80132 NAPOLI

C O N T R O

A[redacted] A[redacted] SPA, rapp.to e dif.so dall'Avv. DE MATHIA MARIO nonché dagli avv. Enzo Morrico e Valeria Cosentino , presso il primo domiciliata come da procura in atti in VIA G.MARTUCCI N.56 80121 NAPOLI

osserva:

a.La controversia in esame è trattata con rito sommario speciale, in ragione del disposto di cui all'art. 1 comma 67 della legge 28 giugno n. 92/2012 che stabilisce che " I commi da 47 a 66 si applicano alle controversie instaurate successivamente alla data di entrata in vigore della presente legge

In ragione dell'oggetto della domanda è stato disposto all'udienza del 25 settembre 2013, il mutamento del rito, avendo l'attore intrapreso l'azione con ricorso ai sensi dell'art. 414 c.p.c.; ad avviso del giudicante la scelta errata del rito non comporta inammissibilità, pur se tale soluzione è astrattamente prospettabile, in ragione del generale principio di principio di conservazione che impone al giudice, in presenza di un errore sul rito, di non azzerare il processo, ma di adottare i provvedimenti necessari per consentirne la prosecuzione e di pervenire ad un provvedimento di merito. Principio generale che sicuramente viene rafforzato dalla finalità acceleratoria che guida il legislatore della riforma in esame (cfr. App. Roma 18.12.13 est. Di Paolantonio).

b.Il fatto e le domande:

Con ricorso ex art. 414 c.p.c. l'epigrafato ricorrente, ha convenuto in giudizio la A[redacted] A[redacted] spa, per sentire accogliere le seguenti domande: "Accertare e dichiarare la nullità, l'illegittimità, l'invalidità e l'inefficacia del licenziamento intimato a M[redacted] con lettera del 16.2.2012 in ogni caso annullarlo e dichiararlo inefficace; per l'effetto ordinare ad A[redacted] A[redacted] di reintegrare l'attore nel posto di lavoro e condannare la società al risarcimento del danno subito da M[redacted], stabilendo un'indennità commisurata alla retribuzione globale di fatto dal giorno del licenziamento sino a quello dell'effettiva reintegrazione e al versamento dei contributi assistenziali e previdenziali dal momento del

licenziamento al momento dell'effettiva reintegra…"
A sostegno della domanda il ricorrente deduce:
Di aver sempre diligentemente custodito gli strumenti aziendali non divulgando la sua password; Di non aver quindi commesso i fatti che gli sono stati contestati; che la sanzione adottata è nulla in quanto in violazione dell'art. 7 l. 300/70, dell'art. 4 legge 300/70 e della legge sulla privacy, che la sanzione è comunque sproporzionata.
Nel costituirsi la convenuta ha allegato , quanto ai fatti preliminari alla contestazione disciplinare e al licenziamento, testualmente quanto segue:
"il M[redacted] addetto al Supporto operativo e manualistiche) insieme ad altri due suoi colleghi della stessa Direzione, G[redacted] P[redacted] (addetto al Supporto operativo e manualistiche nell'ambito della Direzione Operazioni) e G[redacted] E[redacted] (addetto al Training), attraverso il loro computer aziendale erano, abusivamente, entrati reiteratamente anche nello stesso giorno, nel sistema di altri colleghi, acquisendo illecitamente e-mail personali o riguardanti fatti, notizie e documentazione aziendale di natura riservata;
Ciò è stato possibile in quanto, ogni dipendente, attraverso la WebMail, ha la possibilità di accedere, anche da un PC diverso dal proprio, alla propria casella di posta elettronica, digitando il proprio indirizzo e mail (nome.cognome@[redacted] e la propria password con la conseguenza che, per poter accedere ad una casella di posta elettronica altrui, l'utente deve essere necessariamente a conoscenza della password personale della web mail (altrui) di accesso;
Tutti gli accessi alle caselle di posta in modalità WebMail vengono tracciati in un apposito database di log gestito da ogni singolo server IBM; per cui è possibile risalire ai vari " percorsi " ed ai vari " accessi " da parte e verso tutti i computer dei dipendenti, avvenuti nell'ultimo mese, e verificare, quindi, eventuali accessi non autorizzati di dipendenti in caselle di posta di altri;
attraverso la verifica dei tracciati database di log della webmail, effettuata per il periodo 1.1.2012/2.2.2012 dalla funzione Sistemi Informativi (all.2 - AnalisiWebLogConDHCP_Rev2), sono stati individuati tre indirizzi ip (incluso a quello del ricorrente) che hanno effettuato sistematicamente accessi non autorizzati alle caselle di posta di altri dipendenti;
incrociando tali dati, con quanto risultante dall'analisi dei log del DHCP, è emerso che, nel suddetto periodo, i tre indirizzi ip sono stati assegnati sistematicamente sempre alle tre macchine in uso ai dipendenti P[redacted] E[redacted] e M[redacted] (all. 3 su CD dal file 01 DhcpSrvLog-Thu al file 07 DhcpSrvLog-Wed)
All'esito di tale verifica è emerso che il M[redacted] (al pari di altri suoi due colleghi Esposito e Parisi) aveva effettuato accessi non autorizzati dal 9.1 al 27.1.2012 sulle caselle di posta, tra gli altri, dei seguenti dipendenti : [redacted] (appartenenti alla funzione Risorse Umane), [redacted] (responsabile della Sorveglianza del sito di Capodichino) [redacted] (CFO Pomigliano), [redacted] (Commerciale, Capodichino), [redacted] (Supporto Logistico, Capodichino) e [redacted]

[redacted] *(Help Desk, Capodichino). (come si evince dal sopracitato all. 2)*
in particolare, dipendenti, vittime delle intrusioni, che appartengono alla funzione Risorse Umane, in ragione delle loro funzioni, ricevono via mail corrispondenza inerente all'attività produttiva e documenti aziendali di natura riservata (sull'organizzazione, sugli interventi meritocratici, sulla gestione del personale….);
pertanto, nel corso delle intrusioni, è stata presa illegittima visione e conoscenza di documentazione altamente riservata, quale ipotesi di ricollocazione del personale, piani di interventi retributivi, ordini di servizio in corso di elaborazione. (all. 4 Allegati Riepilogo Rev2)"

Ha poi riportato, la comparente, nella memoria di costituzione, testualmente la contestazione disciplinare, del 8.2.2012, del seguente tenore:

"A seguito delle anomalie verificatesi nell'andamento della rete informatica aziendale, la scrivente Società ha dato incarico ai Sistemi Informativi di controllare la funzionalità della stessa.

Nel corso di tale verifica, peraltro effettuata a campione dalla scrivente Società sui LOG della Web Mail, è emerso che dal PC aziendale a Lei assegnato – AEPWA2L1 – si sono verificate innumerevoli connessioni alla posta aziendale dei dipendenti che di seguito specifichiamo, nelle date indicate (confronta elenco riportato da pagina 5 a pag 12 del ricorso e che qui abbiansi per ristrascritto)Stante il fatto che per disposizione inderogabile aziendale il computer assegnato al dipendente può essere utilizzato, attraverso la propria password - che deve essere e rimanere segreta -, solamente dallo stesso, il quale è peraltro tenuto, laddove dovesse lasciarlo incustodito anche per brevissimi momenti, ad inibirne l'uso disattivandolo, risulta - per quanto sopra rilevato - un utilizzo illecito del mezzo aziendale da parte Sua.

Detto illecito utilizzo Le ha consentito di visionare le mail contenute nelle caselle postali del personale di cui al superiore elenco, compresi eventuali allegati documenti di lavoro riservati.

Gli illegittimi accessi risultano peraltro effettuati durante il Suo normale orario di lavoro.

Tale Suo contestato comportamento, di indubbia gravità, contravviene anzitutto alle norme di comportamento contenute nel vigente Codice Disciplinare ed alle

procedure vigenti in Azienda, le quali, tra l'altro, impongono il corretto utilizzo degli strumenti che sono messi a disposizione dei lavoratori per il fine unico dello svolgimento dell'attività lavorativa.

In più Ella ha, in tal modo, leso la privacy informatica delle summenzionate persone, violando la normativa vigente in materia.

La presente vale come contestazione disciplinare ai sensi degli artt. 7 l. 300/70 e 8 Titolo VII Sezione Quarta del vigente C.C.N.L. Industria Metalmeccanica e della Installazione di Impianti.

Voglia pertanto presentare giustificazioni, preferibilmente scritte entro e non oltre i cinque giorni successivi la ricezione della presente su tutto quanto ha formato oggetto della presente contestazione ed in particolare sui motivi per i quali Ella: a) ha illegittimamente acceduto alla posta elettronica di dipendenti della Società nelle date e negli orari meglio specificati sopra; b) abbia contravvenuto alle procedure vigenti in azienda in materia di utilizzo di beni aziendali a Lei affidati esclusivamente per lo svolgimento di attività lavorativa; c) abbia contravvenuto alle norme riguardanti la privacy delle persone i cui nominativi sono stati sopra specificati; d) abbia svolto tale contestata attività durante l'orario di lavoro, impedendo, per tali contestati interventi, la Sua prestazione lavorativa per la quale riceve la normale retribuzione.

Considerata la gravità degli addebiti che Le vengono mossi, viene altresì disposta nei suoi confronti, ai sensi dell'art. 11 Sezione Quarta – Titolo VII del C.C.N.L. Industria Metalmeccanica e della Installazione di Impianti, con effetto immediato, la "sospensione cautelare non disciplinare".

La scrivente Società, all'esito della procedura disciplinare e dei controlli ancora in corso, si riserva di agire a propria tutela presso le competenti Autorità Giudiziarie, ferma restando la titolarità dei singoli di agire direttamente nei Suoi confronti.

La comparente ha quindi così concluso:

"Voglia l'adito Giudice in via preliminare dichiarare inammissibile il ricorso in quanto non introdotto con ricorso ex art. 1 co 48 legge 92/2012; nel merito rigettare il ricorso ex adverso proposto contro la A[redacted] A[redacted] spa, perché infondato in fatto e in diritto alla luce delle argomentazioni tutte riportate in memoria con condanna dello stesso alla refusione delle spese e competenze di lite.
In subordine, in caso di declaratoria di illegittimità del licenziamento, si chiede che il risarcimento del danno venga ridotto in ragione dell'aliunde perceptum e percipiendum.
In via istruttoria: ci si oppone alla prova testi ex adverso richiesta in quanto inammissibile ed irrilevante in quanto vertente su circostanze generiche e comunque contrarie a documentazione allegata dalla società, in caso di ammissione si chiede di esser abilitati alla prova contraria con i stessi di seguito indicati; si chiede, in caso di contestazione dei fatti allegati alla presente memoria, che vengano ascoltati come testi sui fatti riportati ai punti da 1 a 58 della memoria i sigg.ri: [redacted] salvo indicarne altri, tutti dom presso la società convenuta .
Sin da ora, in caso di contestazione sulla veridicità dei file di log allegati alla memoria si chiede che il giudice voglia disporre accesso presso il data base della società in quanto richiedono il Client Lotus per la loro apertura.
Si chiede in via subordinata disporsi ctu informatica per la verifica dei dati oggetto dell'audit aziendale e sui quali è stata effettuata la contestazione disciplinare."
La domanda appare fondata.
Il datore di lavoro, cui incombe l'onere di provare i fatti costitutivi posti a base del licenziamento ha allegato la descrizione di una complessa fattispecie, facendo riferimento a dati tecnici solo in parte prodotti in giudizio.
In particolare, allegando quale prova della fondatezza del licenziamento documenti informatici sulla cui base è stata effettuata la contestazione disciplinare e il licenziamento stesso, ha chiesto, in caso di contestazione sulla veridicità dei file di log allegati alla memoria che il giudice disponga accesso alla sede della società.
Ha chiesto inoltre, in via subordinata disporsi ctu informatica per la verifica dei dati oggetto dell'audit aziendale e sui quali è stata effettuata la contestazione disciplinare.
Il ricorrente, nella memoria introduttiva, ha contestato la riferibilità degli accessi alla sua persona, negando di averli mai realizzati e contestando l'intera procedura di acquisizione dei dati da parte dell'azienda e la riferibilità alla sua persona e al suo pc.
Aderendo alle richieste delle parti, tenuto conto che l'intera architettura del licenziamento poggia sull'estrazioni dei log dai sistemi che avrebbero consentito all'azienda la individuazione di accessi illegittimi e la loro riferibilità al ricorrente, log in parte prodotti in giudizio, in parte posti a disposizione del giudice presso l'azienda, è stato nominato un CTU. Questi ha, con una relazione tecnica estremamente dettagliata e attendibile, chiarito la natura e la provenienza dei dati prodotti e la natura e provenienza dei dati non prodotti ma

messi a disposizione presso il sistema nativo.
Appare tuttavia il caso di premettere, per una maggiore logicità della decisione, che è fuori di dubbio, ed emerge dalle stesse allegazioni di parte resistente (oltre che incontrovertibilmente dalla lettura dei documenti di contestazione disciplinare e licenziamento) che il lavoratore sia stato licenziato perché ritenuto responsabile "*insieme ad altri due suoi colleghi della stessa Direzione, G[redacted] P[redacted] (addetto al Supporto operativo e manualistiche nell'ambito della Direzione Operazioni) e G[redacted] E[redacted] (addetto al Training), attraverso il loro computer aziendale"* di essere *abusivamente, entrati reiteratamente anche nello stesso giorno, nel sistema di altri colleghi, acquisendo illecitamente e-mail personali o riguardanti fatti, notizie e documentazione aziendale di natura riservata ;*
in particolare è stato ravvisato - *un utilizzo illecito del mezzo aziendale*
è stato così contestato al lavoratore "D*etto illecito utilizzo Le ha consentito di visionare le mail contenute nelle caselle postali del personale di cui al superiore elenco, compresi eventuali allegati documenti di lavoro riservati.*
Gli illegittimi accessi risultano peraltro effettuati durante il Suo normale orario di lavoro.
Tale Suo contestato comportamento, di indubbia gravità, contravviene anzitutto alle norme di comportamento contenute nel vigente Codice Disciplinare ed alle procedure"
Inoltre gli è stato contestato di aver leso "*la privacy informatica delle summenzionate persone, violando la normativa vigente in materia."*
Il licenziamento, per giustificato motivo soggettivo, è stato dunque irrogato perché i fatti di cui alla contestazione disciplinare hanno leso irrimediabilmente il vincolo fiduciario essendo gli accessi imputati al lavoratore (segnatamente di aver "*visionato le mail dei colleghi*").
E' pertanto onere del datore, provare i fatti storici degli accessi e la loro riferibilità al lavoratore.
Ed invero, in termini generali è noto che nell'ipotesi di licenziamento per giusta causa o per giustificato motivo soggettivo – che ha natura ontologicamente disciplinare ed è fondato su mancanze del dipendente tali da costituire, una situazione ostativa alla prosecuzione, anche provvisoria, del rapporto (art.2119 c.c.; art.1 L. n.604/1966) e un notevole inadempimento degli obblighi contrattuali (art.3, prima parte, L. ult. cit.) – la prova fornita dal datore di lavoro deve riguardare, la sussistenza del fatto, la gravità dello stesso, e la sua idoneità ad incidere negativamente sugli elementi essenziali del rapporto (ed in particolare su quello fiduciario) oppure a concretare un inadempimento che, avuto riguardo alle esigenze di tutela del lavoratore (accentuata rispetto a quella generalmente riconosciuta al debitore inadempiente dalla regola della "non scarsa importanza" di cui all'art.1455 c.c), determini una notevole lesione dell'interesse creditorio"
Orbene nel caso di specie il datore, per adempiere al proprio onere probatorio, tenuto conto delle peculiarità del caso, ha fatto riferimento a:

documenti informatici, immateriali, prodotti in giudizio solo in parte su supporto informatico, (essendo chiaro sin dall'inizio che una parte di essi non sono stati prodotti ma messi a disposizione dell'autorità giudicante presso la sede Alenia): i cd. log di sistema.

Ha chiarito il CTU, a pag.2 che si tratta, quando si discorre di log di sistema, di quei " *file in cui sono registrate le attività compiute per esempio da un'applicazione, da un server, o da un interprete di comandi. Ad ogni collegamento sul server, vengono scritte informazioni relative all'accesso dell'utente (Indirizzo IP, data, ora, pagina richiesta, login, account)*

In particolare :

1)I log del DHCP server del sistema Windows Microsoft Server (controllo accesso dei pc sulla rete aziendale) **sono stati prodotti in copia su cd allegato alla memoria**

2) I log del sistema di posta Lotus Domino Server (controllo accesso alle caselle sui sistemi di posta) **sono rimasti custoditi presso l'azienda e messi a disposizione del giudice.**

Questo giudice ha quindi, in particolare, conferito il seguente incarico al CTU:

"il consulente dovrà, eventualmente acquisendo, oltre ai dati informatici contenuti nei cd prodotti, recarsi presso l'azienda al fine di acquisire strumenti per la lettura dei dati forniti ed eventuali dati ulteriori che il datore ha dichiarato di non aver prodotto in ragione della loro dimensione, ma che ha posto a disposizione dell'autorità giudiziaria;

che il CTU dovrà, all'esito della consultazione e lettura dei suddetti dati, fornire dettagliata relazione in ordine al sistema informatico datoriale, per quanto attiene ai fatti oggetto del presente procedimento , e in particolare ripercorrere sulla base dei dati allegati e degli eventuali altri dati messi a disposizione da parte datoriale, in conformità a quanto indicato in comparsa, l'iter tecnico della relazione di cui al documento 2, affinché lo stesso, che involge concetti tecnici sia comprensibile e verificabile dal giudice, ossia accedere ai log di sistema consultabili , come affermato da parte convenuta, tramite l'utilizzo di funzionalità native del sistema di posta elettronica aziendale, basato su software IBM e verificare i presunti accessi anomali nel periodo oggetto di ricorso e riportati nell'elenco di cui all'allegato 2 della memoria;

che, il CTU, svolgerà tali accertamenti chiarendo se gli stessi sono realizzati su file originali o su copie degli stessi e, in tale ipotesi, se i dati siano modificabili o risultino modificabili;

che il CTU analizzerà, inoltre, i files di log del server DHCP (formato nativo) prodotti all'allegato 3, avvalendosi eventualmente del sistema in uso presso l'azienda, chiarendo se gli stessi siano inconfutabilmente o con quale margine di probabilità riconducibili relativi ai files di log del DHCP dal 9/01/12 al 27/01/12;

che, inoltre, chiarirà il CTU, dal punto di vista tecnico, il procedimento in forza del quale è stato ricondotto l'indirizzo ip dinamico di cui alla relazione ispettiva allegata agli atti, alla macchina in dotazione al M[redacted]"

Alla luce della CTU e delle prove in atto occorre dunque valutare, per ritenere se

è raggiunta, la prova degli accessi e che gli stessi siano, come affermato dal datore di lavoro, ricollegabili alla responsabilità del ricorrente in maniera certa, anche attraverso elementi induttivi.
In altre parole prima di tutto occorre scandagliare la ricollegabilità al ricorrente degli accessi, in termini generali e quindi come gli stessi tecnicamente siano realizzati e registrati dal sistema.
Al riguardo è emerso dalla CTU, sotto un profilo squisitamente tecnico:

- che ogni PC ottiene un indirizzo IP (corredato della corretta netmask) dal server DHCP. Il meccanismo di rilascio dell'indirizzo IP è basato sul riconoscimento del MAC address della scheda di rete del PC;

- che l'indirizzo MAC, detto anche indirizzo fisico, è un codice assegnato in modo univoco dai produttori di hardware ad ogni scheda di rete Ethernet o Wireless prodotta al mondo. Il MAC adress è indispensabile per ogni PC, portatile e fisso, che ha necessità di collegarsi ad una rete LAN o ad una rete Wireless e rappresenta un identificativo unico a livello di rete locale. Ad esempio, due schede di rete in due diversi calcolatori avranno due diversi indirizzi MAC, così come avranno MAC address diversi una scheda Ethernet ed una scheda Wireless posizionate nel medesimo computer;

- che ogni MAC address di ogni PC riceve, all'atto della registrazione sulla rete, un indirizzo IP che identifica il PC stesso all'interno della rete locale (LAN). Il meccanismo del sistema Windows prevede che, in linea di massima, venga attribuito lo stesso indirizzo IP al medesimo MAC address presente sulla rete in un certo intervallo di tempo (tempo di lease).

E' stato inoltre chiarito che, all'epoca dei fatti, il PC portatile del Dipendente aveva in dotazione una scheda di rete per il collegamento, via cavo, alla LAN. Ha inoltre il ctu specificato che, sulla scorta delle informazioni desunte dai documenti di consegna e dalle indicazioni dei tecnici, a detto PC era stato assegnato un nome che lo identificava all'interno della rete: AEPWA2ZP.
In buona sostanza era presente una terna di informazioni che identificava il PC ovvero:

1. numero seriale del PC
2. nome macchina assegnato dalle configurazioni al PC
3. MAC address della scheda di rete del PC

L'individuazione del PC sulla rete LAN, però, spiega il CTU, risente di due di queste tre indicazioni. In pratica il server DHCP rilascia sulla base del MAC address l'indirizzo IP dinamico e "pro tempore" al PC.
Ciò che è stato tracciato sui log di accesso riportati nelle documentazioni di processo e sui dati del CD depositato presso il tribunale è la doppia informazione "nome macchina"/MAC Address.

Sulla base di tali enunciazioni diventa possibile comprendere, al giudicante che questo dato, isolatamente considerato, non prova la esistenza di accessi illegittimi né la loro riferibilità al ricorrente.

Ciò che emerge infatti dai dati dei server DHCP è che (come spiegato bene dal CTU):

-al momento dell'accesso alla rete aziendale il PC indicato con "nome macchina" AEPWA2ZP ha lasciato una traccia sul log del sistema Windows Server con funzione di Active Directory e DHCP. (il CTU ha riportato, a titolo di esempio, le stringhe prelevate dai log di cui contenuti delle copie sia sui CD allegati agli atti che sul CD conservato in Azienda che così sono leggibili:

11,01/23/12,08:43:48,Renew,172.31.81.120,aepwa2zp.aeronautica.Alenia Aermacchi.it,001EEC1CB0D2,

32,01/23/12,08:43:57,DNS Update Successful,172.31.81.120,aepwa2zp.aeronautica.Alenia Aermacchi.it,,

11,01/23/12,09:43:48,Renew,172.31.81.120,aepwa2zp.aeronautica.Alenia Aermacchi.it,001EEC1CB0D2,

32,01/23/12,09:43:48,DNS Update Successful,172.31.81.120,aepwa2zp.aeronautica.Alenia Aermacchi.it,

-nei log esiste una corrispondenza tra il nome macchina, appunto il già citato AEPWA2ZP e l'indirizzo MAC 001EEC1CB0D2 proprio del PC in questione

-a fronte di questa associazione il DHCP server ha rilasciato un indirizzo di rete valido. Nel caso in questione:

- 172.31.81.120

da qui l'associazione tra l'assegnazione del PC al Dipendente in questione con uno specifico Indirizzo IP. Nel caso il su citato 172.31.81.120.

La circostanza sin qui esplicata, ossia che i log in discorso riconducano all'indirizzo ip ma non agli accessi illegittimi, era del resto ben chiara all'azienda convenuta, che infatti ha fondato il licenziamento non su questi log, ma sul loro "incrocio" con gli altri log, del secondo tipo sopra riportato, non prodotti ma messi a disposizione del giudicante.

Ed infatti se il collegamento di quell'indirizzo iP agli indirizzi di posta elettronica dei dipendenti "spiati" (es. [redacted]) non emerge dai log prodotti in giudizio su cd, ossia i log dhcp, è proprio l'incrocio dei dati scaturenti dai quei log con i diversi log del sistema Lotus Dominio (non prodotti ma posti a disposizione) a fornire il tassello mancante del mosaico, consentendo di ricondurre gli accessi al computer e quindi (presumibilmente) alla persona del ricorrente.

Diventa allora fondamentale, per poter ritenere provati i fatti allegati dal datore di lavoro, ossia scaturenti dall'incrocio dei due tipi di log che riconducono gli accessi al computer del ricorrente e quindi presumibilmente al ricorrente, comprendere la natura e l'attendibilità dei dati informatici posti a base del licenziamento.

E di tale valutazione squisitamente tecnica, natura e attendibilità, provenienza e affidabilità, e segnatamente immodificabilità e, per tale via, incontrovertibile riferibilità al pc in uso al ricorrente, è stato incaricato il ctu.

Appare il caso di premettere, in particolare, che tale valutazione si è resa necessaria in quanto i dati informatici posti a base del licenziamento, i log, appunto, non sono più residenti nei sistemi nativi, pacificamente (fatto allegato dalla stessa resistente e scaturente dalla documentazione prodotta); tali log originali in altre e più semplici parole non sono più disponibili, a distanza di tempo dai fatti, mentre sono disponibili solo delle copie degli stessi realizzate dal datore di lavoro, autonomamente, e poste a base del licenziamento

Ha chiarito sul punto tecnicamente il ctu che, "In pratica all'epoca dei fatti fu fatto un accesso amministrativo a detti log e ne furono prodotte copie che poi sono state salvate su un supporto (nella fattispecie un CD) conservato in una cassaforte dello stabilimento di Pomigliano.

Dal punto strettamente tecnico, quindi, i log sono stati "trasportati" al di fuori del sistema nativo sia Windows sia IBM. La ragione di ciò risiede nelle politiche di conservazione e storicizzazione dei log di sistema. Per entrambi gli ambienti di cui sopra, la memorizzazione dei log avviene a "ricopertura": una volta esaurito lo spazio a disposizione per la memorizzazione dei vari log, si procede, per l'appunto, a ricopertura di quelli più vecchi. Per questa ragione il personale tecnico dell'A[redacted] A[redacted] ha ritenuto utile trasportare al di fuori dei sistemi, mediante copia, i file di log relativamente ai fatti dell'epoca per evitarne la perdita."

Tale organizzazione è conforme alla normativa, ha chiarito il ctu nella nota 2 riportando il dato normativo, delle Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) e successive modificazioni che prevede la conservazione dei log degli accessi in maniera inalterabile per un massimo di 6 mesi.

Ha chiarito poi il ctu che la scrittura dei log avviene all'interno dei sistemi con logiche proprie.

Ad esempio i log di sistema per il DHCP server sono memorizzati all'interno dell'"Event Viewer" di Windows. Detti log possono essere esportati/copiati attraverso un file di testo che è "apribile" e quindi consultabile e quindi alterabile con un normale strumento di edizione (notepad ad esempio).

Per i sistemi Domino i log sono memorizzati all'interno del database del sistema. Anche in questo caso i log del sistema possono essere esportati/copiati, ma, diversamente al punto sopra, detti log vengono resi in formato nativo (formato nsf). Per la consultazione è necessario l'uso di uno strumento software, nel caso particolare, un client Lotus Notes dotato delle opportune credenziali di acceso.

Conclude dunque il CTU che, in sostanza, al momento della verifica presso l'Azienda, è stato possibile recuperare solo una copia dei log e non è stato possibile verificarne la conservazione sui sistemi di origine.

La relazione tuttavia, ha chiarito che i dati non hanno quelle caratteristiche tecniche tali da risultare attendibili.

Ed infatti, afferma il ctu, con considerazione che si condivide completamente che **"**Il punto cruciale" non è la circostanza che i log originali siano stati sovrascritti ma la conisderazione circa le le "*modalità di conservazione dei dati per l'incidente di sicurezza appurato dall'Azienda nelle date di cui sopra."*

Osserva il ctu, in definitiva, che pur potendosi prospettare in astratto varie modalità di conservazione dei dati che avrebbero inconfutabilmente determinato la loro immodificabilità e attendibilità, le stesse non sono state adottate dal datore di lavoro.

In particolare :

- con riguardo ai log DHCP (ossia quelli che ricollegano al pc del ricorrente l'indirizzo ip) il ctu ha osservato

Il DHCP server produce file di log in formato nativo sul sistema. Tali log, nel momento in cui vengono "trasportati" al di fuori del sistema, sono memorizzati in file di formato testo, come risulta dai riscontri raccolti. Nel momento in cui si è stata effettuata la copia, il contenuto dei file non è stato sottoposto a nessun controllo di integrità che ne avesse potuto sancire l'identità assoluta con il dato nel suo contenuto originale, così come prodotto dal sistema. In sostanza, per stabilire la congruenza effettiva, **il sistema avrebbe dovuto produrre log firmati digitalmente e marcati temporalmente. Solo in questo caso si sarebbe potuta stabilire l'esatta identicità con il dato originale.**

In assenza di tale attenzione, e considerando che il file copiato è in formato testo, diventa consistente la possibilità di alterazione del contenuto del file. In altre parole nulla è possibile avanzare circa la inconfutabilità del contenuto del file di log.

Con riguardo al secondo tipo di log (ossia quelli che collegano l'indirizzo Ip agli accessi illegittimi) ha osservato il ctu:

Anche il mail server produce file di log in formato nativo sul sistema. Tali log, nel momento in cui sono stati "trasportati" al di fuori del sistema, sono stati memorizzati in file proprietari (file con estensione *.nsf) come risulta dai riscontri raccolti. Anche in questo caso, nel momento in cui si è stata effettuata la copia, il contenuto dei file non è stato sottoposto a nessun controllo di integrità che ne avesse potuto sancire l'identità assoluta con il dato nel suo contenuto originale: vale a dire assenza di firma e marcatura temporale. **In questo caso, però, la struttura del dato nella sua complessità è tale che, anche se non è possibile stabilirne la congruenza effettiva con i dati nativi, è possibile avanzare l'ipotesi di una bassa probabilità di alterazione del dato copiato.**

Comunque ed in ogni caso, conclude il CTU, anche se una parte dei dati risente di una bassa probabilità di alterazione, il processo di ricostruzione è contaminato da una sostanziale confutabilità di ogni elemento.

Orbene è su questo punto che l'impianto probatorio mostra tutta la sua inconsistenza, non avendo provveduto il datore di lavoro a fornire dati attendibili e quindi non avendo adempiuto al proprio preciso onere che certo non muta nella sua essenza in ragione del tipo di documenti o dati da esaminare.

Ed infatti tutti e due i tipi di log sono andati distrutti nei loro originali in quanto pacificamente sovrascritti, non conservati nel sistema di archiviazione.
Le copie degli stessi non sono state estratte con modalità tali da garantirne, in caso di contestazione, la attendibilità e provenienza e la immodificabilità, né cristallizzati "giuridicamente e processualmente in altro modo (ctu preventiva, atp, etc).
Tutto il giudizio si basa dunque su copie, giuridicamente non attendibili, o della cui attendibilità che scaturirebbe dalla conformità degli stessi ad un originale non più esistente, è lecito dubitare in presenza di contestazione da parte del lavoratore, e in relazione alle osservazioni svolte dal CTU.
Spostando il ragionamento tecnico su un piano meramente processuale appare corretto affermare che, essendo l'onere della prova in capo al datore di lavoro, ed essendo il datore di lavoro privo di documenti di provenienza e attendibilità certa , ed anzi essedo emerso dalla miglior scienza ed esperienza che i documenti prodotti sono alterabili almeno quelli che fanno riferimento al ricorrente , ed essendo inutili i secondi in assenza dei primi, appare non adempiuto l'onere probatorio del datore, perché nemmeno vi sono sufficienti elementi indiziari che consentano di pervenire alla prova in via presuntiva.
Pertanto la domanda del ricorrente deve essere accolta, essendo pacificamente applicabile al licenziamento in parola l'art. 18 l. 300/1970 vigente all'epoca del licenziamento.
Il ricorrente deve essere dunque reintegrato sul posto di lavoro come da dispositivo.

Le spese seguono la soccombenza.

PQM

IL TRIBUNALE DI NAPOLI, nella persona del giudice d.ssa Antonella Ciriello

dichiara l'inefficacia del licenziamento intimato a M[redacted]P[redacted]e per l'effetto ne ordina la reintegrazione nel posto di lavoro;

- condanna il resistente al pagamento in favore del ricorrente del risarcimento del danno, commisurato alle retribuzioni globali di fatto (retribuzione lorda di riferimento €2492,80) dal dì del licenziamento a quello di effettiva reintegra, oltre interessi legali e rivalutazione dalle singole scadenze al saldo;
- condanna la convenuta al pagamento degli oneri previdenziali dal dì del licenziamento all'effettiva reintegra;

condanna la convenuta al pagamento delle spese processuali, liquidate in complessive € 2.864.000, oltra accessori;

Napoli li 29.4.2014

Il giudice
d.ssa Antonella Ciriello