Tribunale Napoli, sez. lavoro, Ordinanza 29/04/2014

L'ordinanza analizza il valore probatorio dei *file* di *log*, con le relative operazioni di conservazione ed estrazione, sancendo, anche per il diritto civile e non solo per quello penale, il principio dell'inattendibilità probatoria delle semplici copie di prove digitali.

di Elena Bassoli

LE *BEST PRACTICES* SULL'ATTENDIBILITÀ DELLA PROVA DIGITALE ENTRANO ANCHE NEL GIUDIZIO CIVILE

Elena BASSOLI, *avvocato di diritto e nuove tecnologie, è docente di "Diritto della comunicazione elettronica" presso l'Università di Genova, nonché del Master Universitario di II Livello in Cyber Security and Data Protection, presso il DIBRIS (Dipartimento di Informatica, Bioingegneria, Robotica ed Ingegneria dei sistemi) Unige, autore di oltre 150 pubblicazioni in materia dal 1995 ad oggi, è Formatore per il Ministero di Giustizia e già per il Ministero dell'Interno. E' presidente nazionale ANGIF (Associazione nazionale giuristi informatici e forensi) e CSIG-Genova (Centro studi informatica giuridica).*

1. Introduzione

Con questa ordinanza del Tribunale di Napoli[1], che potrebbe essere definita"epocale", la giurisprudenza lavoristica si accorge dell'inattendibilità delle prove digitali acquisite senza il rispetto di procedure che ne garantiscano l'affidabilità, l'inalterabilità e l'originalità.

Il caso prende avvio da un ricorso presentato da un lavoratore che si ritiene ingiustamente licenziato, per giustificato motivo soggettivo, e chiede il reintegro sul posto di lavoro, nonché il risarcimento del danno. La società, datrice di lavoro, si difende introducendo nel giudizio copie di *file* di *log* del sistema aziendale che proverebbero, a suo dire, che il dipendente si fosse introdotto abusivamente in alcuni *account e-mail* aziendali attribuiti ad altri dipendenti, prendendo così cognizione di contenuti a lui non diretti[2]. La pronuncia, sotto il profilo probatorio, potrebbe quindi avere le medesime ripercussioni della ormai nota sentenza della Cassazione che sancì definitivamente l'inattendibilità del contenuto delle buste raccomandate a/r postali[3]. L'azienda, al fine di provare l'indubbia riconducibilità di tali accessi abusivi al dipendente licenziato, aveva prodotto in giudizio un CD contente copia dei *file* di *log* relativi al controllo di accesso dei PC al *server* aziendale e aveva offerto in prova direttamente al Giudice gli altri *log*, residenti sul sistema informatico aziendale, comprovanti l'accesso agli *account e-mail* altrui. **Il punto nodale della vicenda appare quindi l'errata riferibilità degli accessi illegittimi al lavoratore, essendo invece l'azienda certa proprio della bontà del substrato probatorio offerto in giudizio**.

2. Il sistema aziendale di posta elettronica

L'azienda in questione attribuiva ad ogni dipendente la possibilità di accedere alla propria casella postale anche da un PC, diverso dal proprio, attraverso la *Web Mail*, semplicemente digitando *username* e *password*. Ciò naturalmente implicava che l'intruso fosse a conoscenza di tali due elementi dei colleghi. Tutti gli accessi alle caselle postali in modalità *Web Mail* venivano poi tracciati in un *database* dedicato contenente i *file* di *log*, gestito da ogni singolo server, per cui era possibile risalire ai vari percorsi e accessi da e verso tutti i PC dei dipendenti nell'ultimo mese. Attraverso la verifica dei tracciati dei *file* di *log* della *Web Mail* sono stati individuati 3 indirizzi IP (attribuiti al ricorrente e ad altri due dipendenti anch'essi licenziati) 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 licenziati.

3. La contestazione dell'azienda

L'azienda attribuisce al dipendente l'illegittimo accesso a *e-mail* aziendali di altri soggetti con correlata violazione delle norme di comportamento contenute nel 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. Inoltre viene contestata la lesione della privacy informatica delle summenzionate persone, violando la normativa vigente in materia.

4. La natura dei *file* di *log*

I *file* di *log*, così come descritti all'interno della CTU sono 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, per la fattispecie che qui ci occupa, il CTU ha individuato :

1) i log del DHCP *server* del sistema Windows Microsoft Server (controllo accesso dei pc sulla rete aziendale) che 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) che sono rimasti custoditi presso l'azienda e messi a disposizione del giudice.

5. *La fase istruttoria*

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 su un CD contenente solo alcuni *file* di *log*. 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, dal canto suo, 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 l'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 sia dei dati prodotti, sia dei dati non prodotti ma messi a disposizione presso il sistema nativo aziendale.

6. *La Consulenza tecnica d'ufficio*

La Consulenza Tecnica d'Ufficio, in questa causa, ha avuto senz'altro un'importanza decisiva per il corretto inquadramento del problema. In particolare è riuscita ad evidenziare e chiarire al giudice la totale inattendibilità di dati digitali prodotti in giudizio senza garanzie di inalterabilità e di conformità all'originale.
Per fare ciò il Consulente è partito da alcune nozioni tecniche fondamentali, concentrandosi sul sistema aziendale e rilevando 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; 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 *address* è indispensabile per ogni PC, portatile o fisso, che ha necessità di collegarsi ad una rete LAN o ad una rete Wireless e rappresenta anche un identificativo unico a *live*llo di rete locale.
Di conseguenza 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*). È stato inoltre chiarito che, all'epoca dei fatti, il PC portatile del Dipendente licenziato aveva in dotazione una scheda di rete per il collegamento, via cavo, alla LAN. Inoltre il CTU ha sottolineato 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, vale a dire**:

— numero seriale del PC
— nome macchina assegnato dalle configurazioni al PC
— 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.

7. *Prova digitale: la quadratura del cerchio*

Sulla base di tali assunti diventa possibile comprendere che questi dati, isolatamente considerati, non provano in maniera certa la esistenza di accessi illegittimi né, tantomeno, la loro riferibilità al ricorrente. Che i *log* in discorso riconducano all'indirizzo IP, ma non provino gli accessi illegittimi, era del resto ben chiaro all'azienda convenuta, che infatti ha fondato il licenziamento non su questi *log*, ma sul loro "incrocio" con gli altri *log*, quelli nativi residenti sul *server* aziendale. **Diventa allora fondamentale**, per poter ritenere provati i fatti allegati dal datore di lavoro, vale a dire 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**.

Ora, poiché pacificamente, così come ammesso dalla stessa società, i dati informatici posti a base del licenziamento, non sono più residenti nei sistemi nativi, mentre sono disponibili solo copie unilateralmente formate dal datore di lavoro, risulta di tutta evidenza la loro inattendibilità.
Per entrambi gli ambienti la memorizzazione dei *log*, infatti, 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'azienda ha ritenuto utile trasportare al di fuori dei sistemi, mediante copia, i *file* di *log* relativamente ai fatti dell'epoca per evitarne la perdita.

A ben vedere tale prassi aziendale appare compatibile con la disciplina della tutela dei dati personali[4] che prescrive la sovrascrittura dei dati e la cancellazione di quelli non più necessari entro 6 mesi dall'acquisizione del dato. Ma non basta.
Infatti acutamente osserva il CTU, 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. Come dire "*va bene conoscere e applicare la normativa sulla privacy, ma sarebbe opportuno avere anche nozioni di digital forensics sulla corretta acquisizione della prova digitale*".
In relazione al primo tipo di *file* (quelli che ricollegano al PC del ricorrente l'indirizzo IP) l'unica soluzione sarebbe stata far sì che il sistema producesse *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*.
Con riguardo al secondo tipo di *log* (quelli che collegano l'indirizzo IP agli accessi illegittimi) ha osservato il CTU che 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.**Tuttavia, benché vi sia una bassa probabilità di alterazione, il processo di ricostruzione è contaminato da una sostanziale confutabilità di ogni elemento. Ed 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 entrambi i tipi di *log* sono andati distrutti nei loro originali in quanto pacificamente sovrascritti, mentre le copie degli stessi non sono state estratte con modalità tali da garantirne, in caso di contestazione, l'attendibilità, la provenienza e l'immodificabilità, né sono stati cristallizzati "*giuridicamente e processualmente in altro modo*" (CTUpreventiva, 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 essendo 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.
Tale pronuncia, dunque, appare esemplare per avere adottato un'argomentazione rigorosa che valorizza correttamente le caratteristiche dei dati informatici considerati, attribuendo agli stessi la relativa attendibilità e collegando a quest'ultima la valutazione del valore probatorio degli stessi.

8. Conclusioni

Il commento alla pronuncia giudiziale potrebbe così dirsi concluso, con una vittoria evidente di coloro che da anni si battono nelle aule di tribunale, e non solo, per una seria e decisa presa di coscienza sui rischi insiti nell'allegazione di prove digitali, ma così non è. **Pur nella sua quasi perfezione l'ordinanza evidenzia due coni d'ombra che meritano di essere indagati, non per trovare risposte, ma semmai, per porre ulteriori quesiti**.

La prima "macchia" nella pronuncia è squisitamente procedurale e attiene, ancora oggi, alla necessità, per un giudice, di doversi affidare ciecamente ad una CTU, seppur magistralmente redatta, per arrivare a conclusioni che dovrebbero apparire ovvie ai più e che invece sono misconosciute sia in ambito giudiziario, sia forense, se è vero, come è vero, che esistono ancora condanne penali che si basano su prove digitali acquisite in maniera a dir poco approssimativa, o se vengono ancora emessi decreti ingiuntivi sulla base di semplici stampate di *e-mail*.
Il secondo "neo" concerne le possibili soluzioni alternative per l'acquisizione corretta della prova digitale aziendale nel giudizio *de quo*, espresse dal CTU e fatte proprie dall'ordinanza. Nel passaggio riguardante "*il come l'azienda avrebbe dovuto acquisire le prove*", non viene fatto alcun riferimento alle reali tecniche di acquisizione della prova digitale, come espresse nelle *best practices* internazionali in materia, richiamate dalla L. 48/2008[5].
Qui infatti il CTU si limita ad affermare che sarebbe stato sufficiente apporre una firma digitale e una marca temporale, per dare certezza alla prova inerente ai *file* di *log*. Ma così non è. **Infatti anche una firma digitale e una marca temporale, in mancanza di possibilità di *matching*** (attuabile solo con un'acquisizione ad esempio tramite un *write blocker*[6] e il calcolo dell'*hash*[7]) con i *file* originali, avrebbe semplicemente attestato che in quel dato momento il datore di lavoro aveva acquisito dei *file*, senza dare conto se essi fossero stati manomessi prima dell'apposizione di firme e marcature temporali. Qui sarebbe occorso andare oltre, riuscire cioè a dare prova dell'inalterabilità del dato copiato rispetto al dato originale dei sistemi, il che, senza un dato originale da confrontare con la copia in corso di giudizio, risulta impossibile.

Apprezzabile in questo senso è invece il tentativo di "correggere il tiro" suggerendo la necessità di un accertamento tecnico preventivo o di una consulenza tecnica di parte *ante causam*, non con la semplice apposizione di firma e marcatura[8]. ©

NOTE

1. Ord. Trib. Napoli, 29.04.2014.
2. In particolare "le vittime", appartenevano alla funzione Risorse Umane, e in ragione delle loro funzioni ricevevano via e-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, quali ipotesi di ricollocazione del personale, piani di interventi retributivi, ordini di servizio in corso di elaborazione.
3. Il riferimento è qui alla nota sentenza Cass. civ. 12.5.2005 n. 10021.
4. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).
5. Legge 18 marzo 2008, n. 48, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 – S. o. n. 79.
6. A titolo approssimativo si può affermare che il write blocker ha lo scopo di assicurare che durante la copia la memoria di massa sorgente (reperto originale) non venga in nessun modo alterata dalla scrittura di dati, a prescindere dal fatto che siano dati dell'utente o dati di sistema/file system.
7. Tale stringa rappresenta l'impronta digitale del contenuto in chiaro e se questo venisse alterato anche in minima parte, la sua impronta non corrisponderebbe più a quella effettuata in precedenza. Quindi due sequenze di input identiche generano lo stesso codice hash, due sequenze diverse generano codici hash diversi.
8. Se la procedura è corretta ed il write blocker opera nel modo migliore ci si aspetta che il valore dell'hash dell'immagine e quello della memoria di massa sorgente (prima della copia) risultino, a fine processo, identici. ◊