Cristina Vicarelli
Avvocato

File di log: se la privacy non basta

L'Ordinanza resa dal Tribunale Napoli in data 29.04.2014 affronta un tema che sarà sempre più attuale, a mano a mano che le procedure di automatizzazione e informatizzazione, già ampiamente utilizzate nelle imprese, avranno necessità di essere tradotte nel processo a supporto delle contrapposte istanze.

Ciò che gli operatori notano da qualche tempo, infatti, è la forte **disgregazione normativa**, che porta il documento informatico ad essere oggetto di diverse discipline, che se non vengono sapientemente integrate tra loro possono incagliare le imprese tra la secche di adempimenti tanto complessi quanto inutili.

Nel caso di specie il Tribunale si trovava a decidere circa il licenziamento di un dipendente accusato di essersi introdotto abusivamente nelle caselle di posta dei colleghi, venendo a conoscenza anche di informazioni riservate dell'azienda alle quali non avrebbe potuto legittimamente accedere.

I file di log

La prova della condotta posta a fondamento del licenziamento veniva fornita dal datore di lavoro attraverso riscontri tecnici: essa si traeva dal confronto incrociato tra **i file di log di accesso del pc alla rete aziendale** (che venivano riversati in giudizio su supporto ottico) e i **file di log di accesso alle caselle sui sistemi di posta,** che venivano posti a disposizione del Giudice presso l'Azienda.

Le conclusioni alle quali era pervenuto il datore di lavoro erano fortemente contestate dal lavoratore licenziato. Il Giudice, pertanto, affidava al Consulente tecnico di ufficio il compito di valutare la prova, trovandosi nella necessità di **determinare la natura e**

l'attendibilità, la provenienza l'affidabilità e l'immodificabilità dei dati informatici posti alla base dell'impugnato licenziamento.

Solo attraverso la verifica delle caratteristiche sopra elencate sarebbe stato possibile riferire in maniera incontrovertibile gli accessi contestati al pc del dipendente, e, grazie al sistema rigido di assegnazione e gestione delle credenziali vigente in azienda, al dipendente stesso.

La disciplina privacy

Dalle informazioni che si ricavano dalla pronuncia il datore di lavoro pare aver applicato scrupolosamente la disciplina in materia di privacy, e aver diligentemente osservato tutti i necessari adempimenti. L'impostazione del giudizio gli appare, *prima facie*, favorevole.

Il consulente tecnico d'ufficio verificava che i file di log non venivano conservati sui supporti nativi: essi erano stati **"trasportati" fuori dal sistema originario in ossequio alle procedure adottate in azienda per la conservazione e storicizzazione dei log di sistema**. La memorizzazione dei log avveniva "a ricopertura": una volta esaurito lo spazio a disposizione per la memorizzazione dei vari log si procedeva alla ricopertura di quelli più vecchi: per questo il personale dell'azienda riteneva di dover provvedere a trasportare fuori dai sistemi i log riferiti all'epoca dei fatti, **mediante copia**: per evitarne la perdita. Il CTU osservava che la procedura era **conforme a quanto disposto dal Garante per la protezione dei dati personali** nel provvedimento **in tema di amministratore di sistema** del 27 novembre 2008 e s.m.i. (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) che prevede la conservazione degli accessi in maniera inalterabile per un massimo di sei mesi. Tutto parrebbe volgere al peggio per il lavoratore licenziato: ma, come si dice, il diavolo si nasconde nei dettagli...

Integrità dei file di log

Infatti, come si è accennato sopra, vi erano due tipologie di file di log: gli uni (relativi alle caselle di posta) erano stati esportati nel database del sistema stesso, avevano mantenuto il **formato originario (nsf)**, ed erano consultabili attraverso uno specifico software e con l'impiego delle necessarie credenziali di accesso, gli altri (relativi all'accesso del pc alla rete aziendale), invece, inizialmente memorizzati all'interno del visualizzatore eventi di windows, **erano stati copiati attraverso un file di testo** - che, come è noto, può essere aperto con qualunque editor di testo ("blocco note", per esempio).

Per il CTU (e per il Giudice che ne condivide le conclusioni) il problema non è tanto che i file originari siano andati distrutti e che le deduzioni del datore si basino su mere copie, quanto che **nel momento in cui veniva effettuata la copia il contenuto dei file non veniva sottoposto ad alcun controllo di integrità che ne potesse sancire la conformità all'originale.**

Tuttavia, per i file in **formato proprietario (nsf)** data la loro complessità, anche nell'impossibilità di stabilirne la congruenza effettiva con i dati nativi, appariva **improbabile** che essi fossero stati alterati.

Non così per i file estratti dal visualizzatore eventi di Windows: il **formato file di testo**, unitamente alla possibilità di procedere alla loro apertura con un semplice editor come "blocco note", equivaleva a dire che **con "blocco note" i file potevano anche essere consultati e, di conseguenza, alterati.** Ciò avrebbe reso imprescindibile, nel momento in cui venivano effettuate le copie, il ricorso a strumenti che ne garantissero la identità assoluta con il contenuto originale, e l'inalterabilità nel tempo: effetto che si poteva ottenere, secondo il consulente, solo attraverso l'**apposizione di marca temporale e firma digitale**. Adempimenti che il datore di lavoro, tuttavia, non aveva posto in essere.

Il valore probatorio dei documenti informatici

Il datore di lavoro, perciò, soccombe: egli non è stato in grado di assolvere l'onere probatorio che gli incombeva perché le copie dei log non sono state estratte con modalità tali da garantirne, in caso di contestazione, attendibilità, provenienza e immodificabilità.

La sentenza tocca uno dei nodi dei quali le aziende appaiono meno consapevoli: il valore probatorio dei documenti informatici. Se è vero che il documento informatico non sottoscritto, a norma dell'articolo **2712 cc**, al pari delle altre riproduzioni meccaniche **forma piena prova** dei fatti e delle cose rappresentate, se colui contro il quale è prodotto non ne disconosce la conformità ai fatti o alle cose medesime, è anche vero che i documenti informatici **non sottoscritti sono *liberamente valutabili*** *in giudizio, tenuto conto delle loro caratteristiche oggettive*

- *di qualità,*
- *sicurezza,*
- *integrità ed*
- *immodificabilità* (art. 20 CAD).

Si tratta di un controllo che il Giudice effettua **ex post**, e che, se negativo, non può essere sanato (a meno che non sia il frutto di una valutazione erronea, e come tale impugnabile). Infatti, il documento viene riversato in giudizio senza conoscerne prima il valore probatorio. Occorrerà allora **essere molto attenti nella fase di formazione della prova**, perché, come dimostra la pronuncia in commento, in assenza di apposizione di firma digitale e marca temporale, un formato facilmente alterabile non dà alcuna garanzia. Le imprese (e i professionisti) potranno allora affidarsi alle regole della conservazione digitale per conservare i documenti informatici di loro interesse (o la cui conservazione è imposta per legge: si pensi alla corrispondenza commerciale via pec...) oppure cristallizzare i documenti "giuridicamente e processualmente" attraverso modalità alternative e antecedenti il giudizio vero e proprio (ctu preventiva o atp, ad esempio).

Il rispetto della normativa privacy non garantisce la prova

Tuttavia vi è un altro aspetto che merita di essere evidenziato: il datore di lavoro aveva conservato i file di log nel rispetto delle prescrizioni del Garante Privacy in tema di **amministratore di sistema.**

In particolare il provvedimento prevede al punto 4.5 "**Registrazione degli accessi**" che

"Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di **completezza, inalterabilità e possibilità di verifica della loro integrità** adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi."

In calce il Garante interveniva per rendere chiarimenti, e al punto 12) nell'esplicare le caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log suggeriva, nei casi più semplici, l'eventuale **esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili.**

Tale sistema di conservazione soddisfa la normativa privacy, ma non ha una validità generale: come si nota "*completezza, inalterabilità e possibilità di verifica dell'integrità*" **non sono completamente sovrapponibili a** "*caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità*" che sono i parametri in base ai quali il giudice è chiamato a valutare i documenti informatici. Pertanto, la trasposizione su supporto ottico potrà essere utilmente impiegata per osservare gli adempimenti privacy ed evitare le sanzioni del Garante, ma non potrà certo essere traghettata oltre il suo ristretto e specifico ambito di applicazione assurgendo a regola di conservazione digitale: quest'ultima, infatti, ha una propria, complessa, normazione che non può subire deroghe da parte del Garante Privacy (che simili deroghe, peraltro, nel citato provvedimento, neppure si proponeva).