Il DPCM 13 novembre 2014 ha portato alla ribalta anche nel mondo forense il concetto di "impronta del documento informatico" impiegato, nel caso specifico, come strumento per riferire in modo certo e univoco, come fosse una sorta di "timbro di congiunzione virtuale", l'attestazione di conformità redatta su documento separato agli atti e documenti cui la stessa si riferisce (art. 4 comma 3 e art. 6 comma 3 DPCM 13.11.2014). Ma cos'è esattamente l'impronta di un file? Anzitutto occorre aver ben chiaro cosa sia un file. Non me ne vorranno gli informatici per inesattezze e uso improprio di termini decisamente (e volutamente) poco tecnici.

Cos'è un file?

Per chiarire cosa debba intendersi per "file" immaginiamolo semplicemente come una scatola dove, al suo interno, il nostro computer conserva ogni nostro singolo testo, fotografia, brano musicale che abbiamo salvato, scaricato, ricevuto per mail. Sopra ogni scatola il nostro computer scrive alcune informazioni di servizio come ad esempio il nome del file stesso, la data di creazione della scatola e chi ha il "permesso" di aprirla. Aprendo la scatola immaginiamo di trovare un cordone più o meno lungo di lampadine (bit) che possono essere accese (1) o spente (0).

Come fa il computer a distinguere e dare un senso a questa lunghissima sequenza di lampadine tutte uguali per mostrarle come una foto piuttosto che un testo word o un PDF? Pensiamo ad una ricetta di cucina scritta in inglese: in effetti non è altro che una sequenza di lettere. Lettere che però assumono un significato se raggruppate in parole e frasi. Significato che sono in grado di comprendere se conosco la lingua inglese.

Dunque il computer, conoscendo la lingua (formato) della nostra ricetta (il contenuto del file) è in grado di leggerla e prepararci ciò che è l'oggetto della ricetta stessa (visualizzare una foto, ad esempio).

Ma tornando al contenuto della scatola, di quante "lampadine" stiamo parlando? Così, per avere un'idea, la scansione per immagine di una sentenza di 5 pagine con dimensione 2.029Kb (c.ca 2Mb) contiene oltre 16 milioni di lampadine (bit).

Immaginiamo adesso di dover trasmettere la nostra scatola contenente la sequenza di oltre 16 milioni di lampadine all'altro capo del mondo e dover

verificare con una semplice telefonata al destinatario che nessuna lampadina si sia fulminata nel viaggio. Più precisamente vogliamo essere certi che tutte le lampadine siano arrivate a destinazione così come erano partite ed abbiano mantenuto la stessa identica sequenza accesa/spenta.

Potremmo armarci di pazienza e comunicare al nostro interlocutore lo stato di ogni singola lampadina. Hmm, più di 16 milioni di lampadine... impensabile! Serve qualcosa di più semplice ed efficace. E qui entra in gioco l'hash e l'impronta del file.

Cos'è l'hash?

L'hash è la funzione che consente di ricavare (calcolare) l'impronta digitale di un file (digest) o, meglio, del suo contenuto. Calcolare l'impronta significa cioè affidarsi ad una funzione logico-matematica che partendo da una sequenza di bit di qualsiasi "lunghezza" (come nel nostro esempio le oltre 16 milioni "lampadine" che costituiscono il pdf della sentenza) restituisca una sequenza di pochissime "lampadine", a lunghezza fissa e predeterminata, gestibile anche senza strumenti informatici (tanto da poterla trascrivere a penna anche su un banale foglio di carta). Esistono varie "tecniche" (algoritmi) per calcolare un'impronta come ad esempio il Secure Hash Algorithm 256 (SHA256) che genera un hash-digest (impronta) di 256 bit (apparentemente una sequenza di 64 caratteri che in realtà è una "rappresentazione raggruppata" delle nostre 256 lampadine, mi perdoneranno gli informatici).

La funzione deputata alla generazione dell'impronta (hash) deve garantire essenzialmente:

1. che non sia possibile eseguire l'operazione inversa di ricavare dall'impronta la sequenza originaria (il file di partenza) né di individuare una qualsiasi sequenza alternativa di bit che possa generare quella stessa impronta;
2. che sia (praticamente) impossibile ottenere impronte uguali partendo da files diversi fosse anche la differenza, come nel nostro esempio, di una sola lampadina sulle oltre 16 milioni della sequenza.

Chiarito questo concetto (hash = funzione per ricavare "l'impronta digitale" di un file) possiamo rispondere alla domanda iniziale: come verificare con una semplice telefonata che la nostra scatola contenente la sequenza di oltre 16

milioni di bit sia arrivata a destinazione senza alcuna alterazione del contenuto? Semplicemente calcolando l'impronta prima della partenza e dettandola al telefono al destinatario della nostra scatola. Questi non dovrà fare altro che calcolare nuovamente l'impronta del file ricevuto e confrontarla con quella che abbiamo dettato al telefono. Se le impronte coincidono i files sono uguali significando che la trasmissione non ha subito alcuna "corruzione".

Questo è soltanto uno degli innumerevoli impieghi della funzione di hash.

Ma torniamo al DPCM 13.11.2014.

Come viene attestata la conformità delle copie cartacee? Spesso con la semplice apposizione di un timbro sulla copia recante la formuletta canonica ovvero con attestazione separata materialmente spillata alla copia stessa e congiunta con un timbro (come per la formula esecutiva).

Bene, come riprodurre in digitale queste due "modalità" di attestazione della conformità? Esattamente come spiegato dal DPCM citato (artt. 4 comma 3 e 6 comma 3):

1. "sovrapponendo" alla copia medesima l'attestazione di conformità proprio come se vi applicassi un timbro (vedasi ad esempio la procedura illustrata dall'Avvocato Giuseppe Vitrani);
2. oppure redigendola su file separato che però dovrà in qualche modo essere congiunto virtualmente alla copia stessa (come per una formula esecutiva).

Ebbene, come faccio a "spillare" l'attestazione di conformità alla copia e mettere un bel timbro di congiunzione? Semplicemente indicando nell'attestazione l'impronta del file da congiungere virtualmente.

L'impronta serve soltanto a questo!

Io che ricevo la copia di una sentenza in formato PDF come faccio a capire se è una copia conforme? Allo stesso modo di come farei se avessi ricevuto una copia tradizionale cartacea. Vado a vedere l'attestazione di conformità.

E questa, trattandosi di documento informatico, potrei trovarla sovrapposta all'immagine stessa della sentenza (come fosse un timbro) oppure come file

separato. In quest'ultimo caso come faccio a verificare che l'attestazione sia virtualmente spillata e congiunta alla copia? Semplicemente calcolando l'impronta della copia e confrontandola con quella indicata nell'attestazione. Se le impronte coincidono significa che quei documenti (copia e attestazione) sono virtualmente spillati l'uno all'altro. Tutto qui.

Copie e duplicati

Il Codice dell'Amministrazione Digitale distingue fra "duplicati" e "copie" ingenerando un po' di confusione atteso che, da un punto di vista informatico, non esiste differenza tra copia e duplicato: due files sono identici o non lo sono. In effetti il concetto di "copia" è mutuato dal mondo analogico.

Ciò risulta evidente con la lettura delle definizioni date dallo stesso CAD secondo il quale la "copia informatica di documento informatico" è il documento informatico "avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari".
Il "duplicato informatico" è invece il documento informatico "ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario".

Quindi occorre tenere distinti quelli che sono il contenuto sostanziale del documento informatico (ad. esempio la sentenza "x") dal contenuto formale (la sequenza di bit o delle nostre lampadine).

Insomma, il duplicato informatico è la copia "bit a bit" di un file, un clone perfettamente identico e indistinguibile dall'originale perché "è" un nuovo originale. Tornando al nostro paragone avremo due (o più) scatole di contenuto assolutamente identico che dunque genereranno impronte identiche. Questo è un concetto che nel mondo analogico, in effetti, non esiste! Neppure due pecore Dolly sarebbero identiche come due files duplicati!

La copia (secondo il CAD) è invece la rappresentazione di uno stesso documento (stesso contenuto sostanziale) ma che dal punto di vista formale costituisce un file "diverso". La sequenza di bit è diversa, le impronte sono diverse. Questo perché è all'interno della scatola che qualcosa è diverso.

Ma cosa esattamente? Beh, possono essere diverse tante cose, in primis i c.d. "metadati", informazioni aggiuntive rispetto a quelle scritte all'esterno della

scatola e che sono invece contenute al suo interno. Come se dentro alla scatola ci fosse una scheda con informazioni e dettagli che durante la copia possono essere aggiornate, integrate, modificate a piacimento senza tuttavia alterare il contenuto "sostanziale".

Per capire: provate a calcolare l'impronta di un testo word che avete già registrato sul vostro computer. Adesso aprite quel documento e scegliete dal menu File -> Informazioni -> Proprietà ->Proprietà avanzate. Avrete la possibilità di modificare moltissimi metadati come ad esempio il nome dell'autore piuttosto che la descrizione del contenuto. Adesso salvate il file e ricalcolate l'impronta. Dato che abbiamo messo le mani dentro alla scatola, pur non cambiando una virgola del testo, l'impronta sarà inevitabilmente diversa.

In conclusione due files le cui impronte coincidono sono esattamente uguali e rappresentano, per il CAD, due duplicati (entrambi originali).

Se due files sono la rappresentazione dello stesso contenuto ma hanno impronte diverse, uno è la copia dell'altro.

Ma attenzione, questo è probabilmente un risultato cercato proprio per poter distinguere originali e duplicati dalle loro copie!

E ciò accade allorchè si scarichi dal pst un documento. Non viene fornito un duplicato ma una semplice "copia" (nel senso inteso dal CAD) ovvero un file "avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari". Per contenuto in questo caso non si deve intendere il nostro cordone di lampadine ma semplicemente cosa questo file mi rappresenta.

Ma tutto questo – come abbiamo potuto verificare e scoprire empiricamente giocando in queste ultime settimane con il calcolo delle impronte sui files ricevuti via PEC dalla cancelleria o scaricati dal pst – nulla ha a che vedere con l'impronta "timbro di congiunzione" di cui al DPCM 13.11.2014

Quell'impronta è solo e necessariamente quella calcolata sulla "copia" che dobbiamo dichiarare conforme.

Un equivoco comune

Qualcuno si chiede se, al contrario, l'impronta da inserire nell'attestazione di conformità non debba essere - ad esempio per l'ipotesi di cui all'art. 6 comma 3 DPCM in parola - quella corrispondente all'originale conservato nel fascicolo informatico. La cosa potrebbe anche avere un senso: indico cioè nell'attestazione l'impronta di quello che è il vero originale informatico del quale ho estratto la copia. Ma attenzione, la norma non dice e non richiede questo! Peraltro in tal caso, anche se e quando il pst mostrerà l'impronta del file originale, come potrei essere certo che quell'impronta è proprio quella dell'originale se non posso scaricarlo? Servirebbe una norma ad hoc ed un nuovo potere di certificazione. Invece la norma tecnica (il DPCM) è chiara e parla esplicitamente di riferimento temporale e impronta "di ogni copia o estratto informatico".

Facciamo un altro esempio "analogico" per chiarire ancora meglio perché l'impronta non può che essere quella calcolata sulla copia cui si riferisce l'attestazione. Senza la spillatura virtuale costituita dall'indicazione dell'impronta sull'attestazione, la notifica della copia di una sentenza estratta dal pst con attestazione di conformità sulla relata sarebbe un po' come se l'ufficiale giudiziario andasse a consegnare al destinatario una copia semplice della sentenza e l'attestazione di conformità su un foglio separato. E' vero che in caso di notifica via PEC io mittente (grazie alla ricevuta di consegna completa) posso sempre dimostrare che quell'attestazione si riferisce alla sentenza allegata nello stesso medesimo messaggio ma questa è un'altra storia...

La norma tecnica (il DPCM in parola) si è preoccupata soltanto di dettare le modalità per riferire in modo certo l'attestazione alla copia proprio come avviene tradizionalmente lavorando con il cartaceo.

Da qui attenzione ad utilizzare correttamente questa sorta di spillatrice virtuale. Poniamo il caso di dover iscrivere al ruolo una procedura esecutiva presso terzi e voler attestare la conformità della copia del pignoramento, del titolo e del precetto con dichiarazione inserita in una nota di deposito (ad esempio con la procedura descritta dell'Avvocato Luca Sileni). Volendo inserire l'impronta dei files (art. 4 comma 3 DPCM) dovrò fare attenzione a firmare con il redattore soltanto il necessario e non i files del pignoramento, del titolo e del precetto sui quali ho precedentemente calcolato l'impronta riportata sulla nota di deposito. Diversamente è un po' come avessi avuto sulla mia scrivania la mia bella copia conforme dei documenti con attestazione sull'ultima pagina. Poi, al momento

del deposito, invece di depositare la copia conforme avessi "staccato" l'attestazione sull'ultima pagina e depositato quella insieme ad una copia semplice degli atti che peraltro avrei inutilmente firmato di pugno….

Infine, in caso di notifica via PEC, come ricordato dalla stessa webapp per la redazione assistita della relata: "… l'impronta deve necessariamente essere calcolata sul file che sarà allegato alla PEC senza che lo stesso venga successivamente modificato/manipolato in alcun modo. In particolare se devi allegare un file firmato digitalmente, ricorda di calcolare l'impronta proprio sul file firmato. Il destinatario della notifica deve infatti essere in grado salvare gli allegati ricevuti con la PEC, calcolarne le impronte e confrontarle con quelle indicate nella relata di notifica al fine di verificarne la corrispondenza …".