Informatica

Quando l'informatica è la tomba del diritto

di Nicola Bortolotti

Il titolo può apparire forte, giacché rasenta senza dubbio la (voluta) provocazione. Tutti coloro i quali abbiano avuto che fare in un'aula giudiziaria con procedimenti che coinvolgessero Computer, collegamenti Internet, moderne tecnologie e affini – siano essi semplici utilizzatori o addetti ai lavori – ben sanno, tuttavia, quanto scivoloso e ricco di insidie possa essere il confidare in una "prova" (o "controprova") – per così dire – "informatica".
Per capire cosa si voglia intendere, non c'è nulla di meglio che presentare – in forma ovviamente anonima – alcuni casi reali, "case history" più o meno dolorosi per le parti in causa, sempre più di attualità in un mondo in cui i rapporti tra persone fisiche e giuridiche sono spesso veicolati dai mezzi elettronici; situazioni nelle quali, a volte, le tracce informatiche non possono concorrere in alcun modo alla costruzione della cosiddetta "verità processuale" e invece – in altri casi – ne costituiscono la imprescindibile base.

La transazione (contestata) via email

Il caso preso ad esempio è una causa da poco più di un migliaio di euro, quasi simbolica, nella quale un fornitore sollecitava un pagamento che la parte attrice rifiutava in quanto il prodotto era a suo dire difforme da quanto richiesto via email; la parte attrice lamentava anche una discordanza tra il prezzo concordato (sempre via email) e – essendo in possesso dell'archivio di posta elettronica – sollecitava una Consulenza Tecnica d'Ufficio atta a chiarificare la cosa, chiedendo inoltre i danni al fornitore.
Come si può facilmente evincere, si tratta di un caso tipico e – proprio per questo – assai eloquente nella sua semplicità, quasi paradigmatico.
Queste le domande poste al CTU dal Giudice di Pace, nonostante il consulente avesse già preannunciato più volte alle parti convenute la situazione di sostanziale indecidibilità nella quale si sarebbe ricaduti:

"Accerti il C.T.U. quale sia stato il messaggio E-mail di ordine degli (...) di cui è causa e del relativo allegato di riproduzione e quale sia stata la data di inoltro"
"Se e quando siano intervenute eventuali modificazioni a detto messaggio e/o allegati"
"Accerti, inoltre, quale sia stato il messaggio ricevuto e la data di ricezione da parte della (...) e se tale messaggio abbia o meno subito modifiche e da chi"
"autorizza il C.T.U. ad accedere ai due computer"

Da notare il fatto – tutt'altro che irrilevante – che la CTU sia stata richiesta nel 2008 a fronte di uno scambio di email avvenuto nel 2005.
Nella Consulenza Tecnica si può leggere, tra l'altro:
In assenza di una infrastruttura di tipo "Posta Elettronica Certificata", [di cui si è parlato e si parlerà ancora su questa rivista, n.d.r] *la validazione di uno scambio di messaggi di posta elettronica, in caso di contestazioni, è possibile unicamente in presenza di riferimenti incrociati e, in particolare:*
- il rinvenimento sul computer del destinatario di un messaggio compatibile con quello memorizzato sul computer del mittente;
- il rinvenimento, sui cosiddetti "log" di attività dei fornitori di servizi Internet (nel seguito denominati provider), di una sequenza di operazioni compatibili con lo scambio di messaggi.
La validazione dei contenuti di uno scambio di posta elettronica comporta un onere e un'incertezza ancor maggiori, in quanto i "log" di attività dei provider non contengono alcuna informazione tramite la quale si possa risalire al contenuto.
Nel caso di validazione di allegati (sotto forma di file), l'incertezza – in assenza di rinvenimento di una corrispondenza perfetta tra l'allegato memorizzato nel computer del mittente e quello memorizzato nel computer del destinatario (cosa pressoché da escludere in caso di contestazione e/o in assenza di tempestive azioni di sequestro) – diviene totale, in quanto è possibile modificare un file (se non firmato digitalmente) in ogni momento e senza lasciare alcuna traccia. [mediante l'utilizzo di programmi più o meno gratuiti alla portata di chiunque, dal classico "touch" del mondo Unix ad utilities sofisticate n.d.r.]
Il caso in esame, fin dall'analisi dei fascicoli, evidenziava una convergenza dei fattori negativi riportati in precedenza, poi confermata dallo studio dei materiali a disposizione. In particolare:
- lo scambio di posta elettronica non è stato effettuato mediante un'infrastruttura PEC

- lo scambio di messaggi di posta elettronica è oggetto di contestazione
- gli allegati sono oggetto di contestazione
- sono passati oltre due anni dal momento del presunto scambio di posta elettronica

Il CTU, nel caso in esame, ha ritenuto superfluo accedere ai *due* computer alla ricerca di riferimenti incrociati in quanto:

"*la parte convenuta (...), per voce del suo C.T.P. (...), ha dichiarato che "il (...) [computer] su cui era sita la mail in questione non è più disponibile in quanto le macchine sono state sostituite, e non mi è stato richiesto un backup della posta". Il recarsi in loco sarebbe dunque stato del tutto inutile, in quanto è impossibile accedere ad un computer (o a un materiale) che non esiste più.*"

Sui messaggi email prodotti dalla parte attrice il CTU ha potuto scrivere:

Di tali messaggi non è in alcun modo possibile garantire l'autenticità in assenza di riferimenti incrociati. Ciò non ostante va rilevato come – senza voler nulla ipotizzare circa la loro effettiva ricetrasmissione, che non può essere provata – essi siano tra di loro coerenti, come evidenziato dalle parti di header riportate in grassetto in appendice.
In particolare: secondo gli header – se autentici, cosa che non può essere né in questa sede né mediante uno o più sopralluoghi presso (...) né affermata né negata – i messaggi B ed E provengono entrambi dall'indirizzo IP (...).
Tale indirizzo, che individua univocamente un utente collegato alla rete Internet, risulta in effetti ancor oggi assegnato, in modo statico, al nodo (...) utilizzato da (...).
Sempre meramente ipotizzando la veridicità degli header, inoltre, il messaggio B risulterebbe in effetti in risposta al messaggio A, così come il messaggio E sarebbe in risposta al D.
Da notare come i files PDF allegati siano nel vetusto formato PDF versione 1.2 (Acrobat 3.x) e sprovvisti sia di qualsiasi tipo di informazione identificativa (che sarebbe comunque modificabile ex post senza lasciare traccia) che della protezione del contenuto tramite password.
Lo studio degli header ha comunque consentito di risalire ai provider di posta elettronica sia della parte attrice che della parte convenuta.
Al fine di tentare una validazione dell'effettiva ricetrasmissione delle cinque mail sopra riportate mediante riferimenti incrociati forniti dai "log" dei provider, si è dunque provveduto a prendere contatto preliminare con (...) [i provider, n.d.r.]. *In entrambi i casi, tuttavia, le risposte ricevute dai provider sono state negative, stante il notevole lasso di tempo intercorso tra lo scambio di email e la richiesta (...).*

Per completezza, questa la risposta del primo provider:

"*(...) non conserva backup della posta quindi, se cancellata dal cliente o scaricata in locale, non vi è alcuna possibilità di recupero. Per quanto riguarda la posta in uscita essa viene gestita dai nostri server solo se il cliente utilizza per tale scopo la nostra webmail o acquista il servizio di SMTP autenticato e rimane comunque valida la regola per cui, se il cliente cancella o non salva i messaggi inviati nella posta in uscita della webmail, di questi non rimane alcuna traccia. Eventuali log di accesso alla webmail delle nostre mailbox possono essere richiesti dall'autorità competente ma sono in nostro possesso solo a partire dal 2006 quando è divenuto obbligatorio conservarli per legge. (...)*"

e del secondo, assai più laconica:

"*(...) Siamo spiacenti ma non siamo più in possesso dei dati da Lei richiesti. (...)*"

da cui il commento del consulente nominato dal Giudice:

Nonostante la coerenza del flusso informativo, non è dunque possibile fornire alcuna prova oggettiva attestante né la effettiva ricetrasmissione né, quel che più conta, il contenuto degli eventuali allegati (aspetto, quest'ultimo, che sarebbe comunque stato indecidibile anche qualora i provider interpellati avessero potuto fornire i dati richiesti)

Il CTU ha effettuato – invano – altri tentativi "alla ricerca degli incroci perduti"; ad esempio:

Stante l'impossibilità di consultare l'archivio di posta elettronica di (...), archivio che – come affermato dal C.T.P. – è stato irrimediabilmente distrutto in seguito alla sostituzione del computer, si è richiesto il supporto CdRom [contenente le specifiche del materiale da fornire, n.d.r.] *citato in alcune parti dei fascicoli (...) Anche se tale data non ha alcun valore probatorio, è comunque facile desumere che non si tratti di un CD fornito da (...)* [parte attrice, n.d.r.] *bensì di un CD masterizzato posteriormente da (...)* [parte convenuta, n.d.r.] *a fini di backup (...) Le immagini in formato Encapsulated Postscript sono riprodotte in appendice. Da notare come, in questo caso, non siano stati masterizzati files in formato PDF, al contrario di quanto era d'uso nei messaggi forniti dalla parte attrice discussi al punto precedente.*

Da cui le conclusioni:

L'analisi condotta mi permette di concludere: relativamente al quesito
- "Accerti il C.T.U. quale sia stato il messaggio E-mail di ordine degli (...) di cui è causa e del relativo allegato di riproduzione e quale sia stata la data di inoltro"
stante l'impossibilità di pervenire alle indispensabili conferme incrociate non è possibile accertare alcunché al proposito, ma solo ipotizzare come verosimile lo scambio di messaggi A-B per quanto concerne la fase di preventivo
Con riferimento al quesito:
- "Se e quando siano intervenute eventuali modificazioni a detto messaggio e/o allegati"
è impossibile esprimersi al proposito.
Infine, al quesito:
- "Accerti, inoltre, quale sia stato il messaggio ricevuto e la data di ricezione da parte della (...) [parte convenuta, n.d.r.] *e se tale messaggio abbia o meno subito modifiche e da chi"*
non solo non è possibile dare alcuna risposta oggettiva, ma allo stato delle cose è anche impossibile ipotizzare un flusso informativo verosimile che possa aver condotto dai files del messaggio D prodotto dalla parte attrice (e si noti che, anche se il verosimile scambio D-E venisse provato, non si potrebbe comunque garantirne l'effettivo contenuto allegato) ai files nel CD masterizzato dalla parte convenuta.
Si ricade, in conclusione, nei classici casi di indecidibilità che caratterizzano il mondo dell'informatica in assenza di riscontri incrociati e laddove non si utilizzino strumenti aventi valore legale, come la posta elettronica certificata e la firma digitale con marcatura temporale.

In altri termini, non solo non si è trovata la desiderata "prova informatica", ma si sono aggiunti ulteriori motivi di confusione ad un caso che presentava già parecchi punti oscuri. Dato il decollo al rallentatore della infrastruttura di Posta Elettronica Certificata (che avrebbe valenza persino superiore a quella di una raccomandata a.r.) situazioni del genere potrebbero verificarsi anche oggi, aggravate dall'endemica lentezza dei procedimenti che rende spesso impossibile l'acquisizione dei dati presso i provider.

Un sito Internet plagiato ma ... sfuggente

Un altro caso emblematico è quello di una contestata violazione di diritto d'autore, con parecchie fotografie di "modelli" scannerizzati da una brochure della ditta concorrente e pubblicizzate via Internet su – addirittura – due siti diversi (comunque riconducibili allo stesso proprietario, seppur con diverso "maintainer").

Il problema che si poneva a Giudice e consulenti, in questo caso, era molteplice, in quanto – stanti i dilatati tempi della giustizia italiana, tali da renderla sovente ingiusta a prescindere dai suoi pronunciamenti – le immagini oggetto del contenzioso erano state nel frattempo rimosse; inoltre, data l'intrinseca natura delle immagini digitali, come poter stabilire in modo oggettivo l'effettivo plagio, visto che sono sufficienti poche operazioni con un software (anche gratuito) di manipolazione delle immagini per renderle estremamente dissimili? A dissipare il secondo dubbio è giunto in soccorso il fatto che, dalle immagini contestate, non era stato rimosso alcun elemento di sfondo, il che le rendeva certamente tratte dalla brochure originale.

Per risolvere il primo problema, il consulente tecnico interpellato dalla parte "offesa" – pur consapevole che una prova diretta e inconfutabile dell'apparizione (e sparizione) delle immagini contese sarebbe potuta scaturire solo dall'analisi dei soliti file di "log" di "FTP upload" del provider che ospitava i siti, ma altresì conscio del fatto che tali files difficilmente avrebbero potuto essere forniti, a causa del tempo intercorso – aveva immediatamente provveduto al cosiddetto "mirroring" dei siti, ovverosia al loro scaricamento integrale mediante appositi software, e successiva masterizzazione per il deposito agli atti. Tale operazione era stata ripetuta, con modalità analoghe, nove mesi dopo.

Per tale operazione era stato utilizzato il software gratuito HTTrack (http://www.httrack.com/), nella modalità "forensic dump" che crea la cosiddetta "forensic image", ossia preserva tutti i dati originali corredandoli di un checksum MD5 e SHA1: in altri termini era stato creato uno "specchio" fedele del sito, idoneo ad essere validato dal Consulente nominato dal Giudice.

La Consulenza Tecnica d'Ufficio ha confermato le previsioni del CTP. In particolare vi si legge:

"*Ai maintainer è stato chiesto l'invio dei file di log c.d. FTP da/verso lo spazio web relativo ai siti di pertinenza (...) La società (...) ha comunicato di non disporre delle informazioni richieste (visto il tempo trascorso dall'epoca dei fatti e vista la legislazione in vigore all'epoca (...) La società (...)* [l'altro provider n.d.r.] *ha comunicato di non disporre delle informazioni richieste (...) L'unico elemento utile ai fini dell'indagine è rappresentato dal cd-rom (...) allegato all'atto di citazione.*

Tale cd-rom è stato creato da (...) [il CTP, n.d.r.] *(sentito anche come teste), in qualità di tecnico esperto in informatica, su incarico della ricorrente. (...)*

È stata verificata la coerenza di tutte le date dell'immagine dei siti ottenute tramite HTTrack, delle date all'interno dei log htslog.txt e new.txt, compresa l'attendibilità delle dimensioni delle immagini scaricate (...)

Per dovere di completezza, trattandosi comunque di un insieme file, è pur vero che è tecnicamente possibile creare un'immagine di un sito con il software HTTrack in un determinato momento e manipolarlo opportunamente in modo da farlo apparire (eseguendo i controlli di cui sopra) in una qualsiasi data del passato. Ma è altrettanto vero che tale operazione è veramente delicata e deve essere fatta con metodicità assoluta. [a questo proposito il CTP aveva anche suggerito di acquisire e far analizzare i propri log di navigazione, presso il suo provider, ma non ve ne è stata necessità, come si vedrà nel seguito, n.d.r.] *Un modo per verificare il contenuto di un sito web nel passato consiste nell'utilizzare una risorsa web denominata Web Archive (web.archive.org) liberamente consultabile sulla rete. (...)*

Analizzando la prima copia di (...) offerta da Web Archive, effettuata il (...), e navigando detto sito così come appariva all'utente all'epoca, ritroviamo una serie di foto che l'attrice asserisce essere utilizzata in modo illegittimo (...).

Alla luce di tale scoperta, ho proceduto con la comparazione del codice sorgente (...) delle pagine (...) ritrovando piena corrispondenza (...) posso decisamente affermare che i contenuti dei siti (...) siano stati nella disponibilità della resistente almeno per il periodo (...)"

Da notare il fatto che, se non fosse stato prodotto un CdRom con il "mirroring" dei siti – costruito in modo tale da poter essere validato dal CTU – e se non fosse stato riscontrato almeno un riferimento "incrociato" su Web Archive – il procedimento anche in questo caso sarebbe, con ogni probabilità, finito nello sgradevole limbo dell'indecidibile, informaticamente parlando.

Stampare non vuol dire protocollare

Si potrebbero citare altri "case history", soprattutto in ambito penale, ma in questa sede è opportuno concludere con un caso "trasversale", visto che tale circostanza viene spesso citata (con riscontri ovviamente negativi) negli interrogatori, ossia la falsa percezione che la semplice stampa di un documento possa lasciare una traccia (più o meno indelebile) sul computer dal quale parte il relativo comando.

È invece il caso di ricordare il fatto che, limitandosi ai sistemi operativi della famiglia Windows (i più diffusi in ambito client), l'unica traccia sul PC è costituita dai cosiddetti "files di spool" (di norma rinvenibili nella directory C:\WINDOWS\system32\spool\PRINTERS). Tali files, tuttavia, vengono – di norma – automaticamente cancellati dal sistema dopo ogni stampa (per evitare un rapido esaurimento dello spazio su disco) salvo il caso – estremamente improbabile – in cui fosse stata precedentemente "spuntata" la casella "Mantieni i documenti stampati" nelle proprietà "Avanzate" della stampante. Per quanto riguarda la connessione di una "pen disk" USB, se ne potrebbe trovare testimonianza nel cosiddetto "registro di sistema" di Windows (HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\DosDevices), ma tale vestigia avrebbe scarso valore, in quanto proverebbe unicamente la connessione, nel passato, di tale dispositivo USB ma non il suo contenuto né l'eventuale avvenuta stampa né, tantomeno, un riferimento temporale oggettivo e incontestabile.