

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO Problematiche di formazione e probatorie

EMAIL, FIRMA ELETTRONICA E FORMA SCRITTA

INTERVENTO NEL CONVEGNO

“DOCUMENTO INFORMATICO: PROBLEMATICHE DI FORMAZIONE E PROBATORIE”

VERONA, 7 MAGGIO 2004

AVV. MARCO CUNIBERTI

Ha suscitato recentemente molto scalpore la notizia di un decreto ingiuntivo, che il Tribunale di Cuneo ha concesso - ex art. 634 c.p.c. - sulla base di una ricognizione di debito contenuta in una normale email, accogliendo la tesi secondo cui, alla luce della normativa in tema di documento informatico, anche la email "semplice" si può considerare sottoscritta con firma elettronica, così soddisfacendo il requisito legale di forma scritta.

L'art. 10, comma 2, del DPR n. 445/00 prevede infatti che *“Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta”*, benchè *“sul piano probatorio il documento stesso è liberamente valutabile”*: pertanto, il documento informatico sottoscritto con tale “firma” è sufficiente quando la legge richieda espressamente la forma scritta per la validità dell'atto (cd. *ad substantiam*) o per la validità di una prova ivi contenuta (cd. *ad probationem*), salve contestazioni sull'autenticità del documento (ma questo riguarda il piano probatorio, per il quale, correttamente, la legge dà al Giudice la più ampia libertà di valutazione).

Di conseguenza, se la normale email contenente la ricognizione di debito si può considerare un documento informatico sottoscritto con firma elettronica, benchè “leggera”, ben potrà allora essere concesso il Decreto Ingiuntivo.

Occorre quindi per prima cosa chiedersi se la email sia un documento informatico, che l'art. 1, comma 1, lett. b) del DPR definisce *“la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”*: ed essendo la email proprio la rappresentazione informatica di tante cose, tra cui una dichiarazione di volontà o di scienza, essa riveste certamente le caratteristiche richieste dalla norma.

Per quanto riguarda, poi, la firma elettronica, l'art. 1, comma 1, lett. cc), stabilisce che questa sia *“l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica”*.

Ora, poichè appare ovvio che la definizione "sottoscrizione" costituisca, per quel che riguarda un documento informatico - e quindi la rappresentazione grafica di dati - una fictio juris (in quanto in nessun caso si sottoscrive materialmente alcunchè, neppure con la firma digitale, che corrisponde

invece all'inserimento, da parte di qualcuno - quasi sempre diverso dall'effettivo titolare - di una smart card e della digitazione di un PIN, che non viene certo riportato nella mail), sembra logico che l'espressione "documento informatico sottoscritto con firma elettronica" possa anche esser interpretata con "firma elettronica apposta (o allegata) al documento informatico".

E' quindi necessario che al documento informatico sia più che altro allegata una firma elettronica, dev'esservi contenuta, in modo che il destinatario se ne possa accorgere.

L'email deve pertanto contenere un insieme di dati in forma elettronica, i quali siano allegati oppure connessi - tramite associazione logica - ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Prima di analizzare la sussistenza o meno di tali requisiti, è opportuno ulteriormente puntualizzare che la norma non chiede assolutamente che questa "firma" sia sicura, certa, infalsificabile: esattamente come la dichiarazione contenuta in un foglietto di carta firmato (che costituisce comunque forma scritta, indipendentemente dal fatto che la firma sia falsa o comprensibile), si richiede solo che questa firma ci sia ed abbia i requisiti di legge.

L'email contiene (oltre eventualmente la firma, "l'indicazione grafica" del mittente, in fondo alla mail stessa, che ai nostri fini non serve ad alcunchè, anche se potrebbe avere rilevanza ai fini penali, ex art. 491 bis c.p.) un indirizzo di provenienza (es. mariorossi@libero.it, che ci dice - a parte il fatto che possa essere falsificata - che essa è o dovrebbe esser stata inviata da un indirizzo creato presso un provider di posta elettronica) e soprattutto gli headers: sono questi una serie di dati precisi, contenenti numerose informazioni (molte più di quante possano esser contenute in uno sconosciuto foglio di carta!), tra cui tutto il percorso della email, l'indirizzo IP di provenienza (cioè a quale utenza telefonica era collegato il computer mittente) e, soprattutto, da quale ISP (Internet Service Provider) provenga.

In pratica, l'insieme di dati indirizzo-headers indica chiaramente che l'email proviene (o dovrebbe comunque provenire) da un'area riservata di un ISP (che cioè, per essere inviata, occorre aver accesso a quell'area riservata), nonché il momento di invio e l'IP, da cui si può risalire addirittura alla macchina che me l'ha mandata.

Passando al secondo requisito, non si può negare che un sistema di autenticazione costituito da un codice per l'identificazione dell'incaricato (username) ed una parola chiave riservata a questo associata (password) costituisca un metodo di autenticazione informatica; l'espressa conferma viene oltretutto dal nuovo Tasto Unico in materia di tutela dei dati personali (DLgs 196/2003), che ha espressamente specificato quanto sopra agli artt. 1 e 2 dell'allegato B.

Come si è visto, l'insieme di dati indirizzo-headers dice che quella data email è stata scritta da qualcuno che ha dovuto (o avrebbe dovuto) necessariamente, per scriverla, inserire un ID e una PW; o, meglio, che chi l'ha scritta, non può non aver inserito un ID ed una PW.

Perciò, grazie al suddetto insieme di dati, si sa che per scrivere quella email è (o avrebbe dovuto essere) stato utilizzato un sistema di autenticazione informatica.

A questo punto, non si può negare che ci sia una connessione logica, un'associazione di idee tra l'insieme di dati indirizzo-headers (contenuti nella email ricevuta) ed il metodo di validazione necessariamente (condicio sine qua non) utilizzato.

Logica conseguenza, a questo punto, è che anche la email "semplice", contenendo tutte le caratteristiche di legge, costituisca un vero e proprio documento informatico munito di firma elettronica (benchè "leggera") e, pertanto, la dichiarazione di volontà o di scienza ivi contenuta rivesta la forma scritta.

In relazione al ragionamento sin qui esposto sono state sollevate alcune interessanti eccezioni, cui sono però state date - quantomeno a parere di chi scrive - soddisfacenti risposte.

In primis, è stato sostenuto che, poiché usando un client di posta (cioè un programma come MS Outlook Express) per inviare una email non viene effettuata alcuna autenticazione (in pratica, per raggiungere il server “dedicato all’invio” del proprio provider, cd. SMTP, al programma non viene richiesta l’immissione di username e password, cosa che invece lo stesso programma effettua automaticamente quando verifica la posta in arrivo), non sussisterebbe la connessione logica con il sistema di autenticazione informatica.

E’ però agevole ribattere che, in primis, così ragionando si ammette implicitamente che la cd. “webmail” (cioè l’invio di posta elettronica accedendo direttamente, via web, al provider che fornisce la casella di posta, non utilizzando alcun programma specifico) ha invece tutti i requisiti, benchè si tratti comunque di una email normalissima.

L’eccezione non reggerebbe inoltre per le email cd. "di risposta" (cioè quelle che rispondono ad un’altra email ricevuta, le quali contengono anche il contenuto della stessa email cui si intende rispondere), ove si è addirittura sicuri che l’autore della risposta è proprio colui che ha ricevuto la prima email, il quale ha dovuto certamente autenticarsi per leggerla (per poi rispondere).

Ma, soprattutto, l’eccezione è infondata anche per il caso di utilizzo del programma di posta: anche se, infatti, non ci si autentica in quella specifica occasione, si utilizza però un identificativo (l’indirizzo del mittente) che si riferisce comunque a un’area riservata, creata apposta e quindi protetta dal suddetto metodo di autenticazione (in pratica, se ci arriva una email dall’indirizzo mariorossi@libero.it, siamo convinti che chi l’ha inviata abbia l’uso esclusivo della relativa area riservata, protetta da un sistema di autenticazione informatica costituito da username e password; in caso contrario - se cioè il mittente inserisse appositamente nel suo client un indirizzo che non esiste, come ad esempio francorossi@libero.it, approfittando del fatto che non è richiesta l’autenticazione e facendo così credere falsamente al destinatario che arriva da quell’inesistente account - commetterebbe un illecito ex art. 491 bis c.p., poiché chiunque crederebbe che quell’account esiste, cioè esista un’area riservata al relativo titolare): pertanto, la connessione logica, l’associazione di idee tra l’insieme indirizzo-headers di quella email e l’utilizzo di dati di autenticazione non viene a mancare, anche se in quel caso concreto non erano stati immessi.

La firma, è infatti costituita dall’insieme indirizzo-headers (che ben sussiste anche nella email inviata dal client), non dall’insieme di dati username-password, cui i primi possono anche soltanto essere “connessi tramite associazione logica”.

Qualsiasi problema si risolverebbe, in ogni caso, adottando un client di posta che effettui l’autenticazione anche per la posta in uscita.

Altro rilievo è stato mosso in quanto, poiché nel caso di webmail l’autenticazione informatica (cioè l’inserimento di username e password) è effettuata prima di scrivere la email e non dopo, non vi sarebbe una vera e propria firma del documento informatico.

Ciò non corrisponde però al vero, poiché - come si è visto - la firma è costituita dall’insieme di dati indirizzo-headers (e non dall’insieme username-password), che viene apposto alla email al momento dell’invio e che deve soltanto essere connesso logicamente al sistema di autenticazione informatica.

In ogni caso, l’eccezione appare di poca consistenza, considerato che, pur parlandosi di “firma” e di “sottoscrizione”, è chiaro che si utilizzi una fictio iuris e ci si riferisca materialmente a qualcosa di diverso.

Per quanto invece riguarda le eccezioni sulla obbiettiva insicurezza della email, la quale sarebbe agevolmente falsificabile, si risponde che il legislatore ha correttamente parlato soltanto di “requisito legale” di forma scritta (così come è in forma scritta anche una promessa di pagamento

scritta sul retro di un biglietto del tram, con in calce una firma qualsiasi), mentre per quanto riguarda l'efficacia probatoria ha lasciato libera valutabilità al Giudice che eventualmente dovesse occuparsi del caso concreto.

D'altronde, gli stessi - se non maggiori - rischi di insicurezza valgono nel caso in cui ci arrivi una lettera cartacea con una carta intestata ed una firma che noi non conosciamo: ebbene, di sicuro è la email, che - ad un'analisi approfondita - può fornirci le maggiori garanzie (si pensi solo a quante informazioni ci sono negli headers, mentre in una lettera si può al limite sapere con certezza da che città è partita).

Le considerazioni sin qui svolte possono rappresentare una svolta nell'attribuzione alla email di un più consono ed adeguato valore legale, anche alla luce del ruolo che ormai tale mezzo di comunicazione riveste: l'invio di email "normali" è infatti oggi il metodo di comunicazione più utilizzato non solo nel commercio elettronico, ma anche nei rapporti commerciali "tradizionali" (tutta la fase precontrattuale e di esecuzione dei contratti - specialmente servizi, appalti, contratti che richiedano continui contatti tra le parti -, gli ordini dei rivenditori ai grossi distributori, ecc., viene fatta via email, lasciando al cartaceo solo la stipula del contratto vero e proprio), per non parlare poi delle specifiche tecniche ed alle comunicazioni interne alle aziende.

Pertanto, in attesa di un'eventuale modifica legislativa, pare corretto sostenere che anche la semplice email soddisfa il requisito legale della forma scritta, pur con tutti i doverosi limiti per quel che riguarda l'efficacia probatoria.