CONTIENE ATTO NOTARILE: PER LA DATA DI SCADENZA VEDERE SUL TAPPO

di **Ugo Bechini**. Da *Federnotizie*, maggio 2001

L'idea che un documento abbia una data di scadenza è estremamente familiare. Che si tratti di una carta di credito, di un certificato di destinazione urbanistica oppure di una procura, un fatto è certo: con la scadenza il documento diviene inidoneo a supportare la nascita di nuovi rapporti giuridici, ferma restando però la validità storica degli atti e dei rapporti sorti durante il periodo di validità del documento.

Ovvio, no? No, non più, con l'avvento della firma digitale. Quando scade il certificato di firma digitale, tutti i documenti sottoscritti durante il periodo di validità della firma stessa perdono rilevanza giuridica. Come scrive Raimondo Zagami (*Firma digitale e sicurezza giuridica*, Cedam, Padova 2000, p. 214) la scadenza della firma produce un effetto corrispondente alla distruzione del documento (*excusez du peu* ...). E la scadenza è eventualità tutt'altro che teorica, visto che la validità di un certificato correntemente non supera i tre anni. Sopravvive, s'intende, il fatto storico dell'avvenuta documentazione, suscettibile di prova, ma il documento informatico in quanto tale è giuridicamente evaporato.

Questo fenomeno, prima facie sorprendente, è ancora di non consolidato inquadramento giuridico, ed alimenta perplessità di vario genere. Occorre però ammettere che il tutto appare meno arcano se solo si pone mente ai meccanismi su cui si fonda la firma digitale (meccanismi peraltro invisibili all'utente, il quale ha a che fare solo con banalissimi pulsanti del tipo "Firma" oppure "Verifica la firma").

Liberamente accessibile in Rete c'è la chiave pubblica di Tizio, che consente a chiunque di accertare se una certa firma è stata apposta davvero da Tizio. Ma da tale chiave pubblica non è (in prima approssimazione) possibile risalire alla chiave privata, quella che consente di creare le firme, e che è gelosamente conservata dallo stesso Tizio. L'intero sistema si fonda su questa singolare proprietà: la chiave pubblica permette di realizzare l'operazione di verifica ma non quella di firma, che pure è perfettamente simmetrica.

Ciò è reso possibile dagli algoritmi che danno vita ai sistemi di firma digitale, le cosiddette one way functions, funzioni matematiche "a senso unico". L'esempio più noto è quello della fattorizzazione, la scomposizione di un numero in numeri primi. Non ci vuol molto a stabilire che 21 = 3 x 7, ma che dire di 92648497 ? Trovare il risultato (7621 x 12157) non è lavoro da poco, mentre l'operazione inversa, anche con la più banale calcolatrice tascabile ad otto cifre, sarà affare di un attimo. Lavorando con numeri composti da centinaia di cifre, come si fa nel campo della firma elettronica, la moltiplicazione resta eseguibile in qualche secondo dal vostro PC, mentre l'operazione di fattorizzazione diviene un compito mostruoso, misurabile in mesi di attività del più potente dei supercalcolatori.

Insomma: l'asimmetria c'è ma non è assoluta. A rigore non è quindi impossibile risalire dalla chiave pubblica a quella privata, usurpando la firma di chiunque altro: è solo un'operazione molto lunga e difficile. Ma quanto lunga? Occorre essere diffidenti. Nel 1977 serissimi scienziati stimavano che il miglior ritrovato dell'epoca, noto come RSA129, richiedesse miliardi di anni per essere violato; quindici anni dopo ad un team di esperti bastarono sei mesi. Simili sorprese non derivano solo dal costante incremento di potenza dei computers ma anche e soprattutto dallo sviluppo di tecniche di criptoanalisi che consentono di semplificare con vari espedienti l'inconcepibile mole di calcoli richiesta da un attacco matematico diretto. Da questo punto di vista l'impiego abituale della firma digitale aumenterà i rischi: disponendo di molti esemplari di firma di un medesimo soggetto, è più facile per un potenziale pirata scoprire la chiave, che ovviamente è sempre la stessa.

Non si può pertanto escludere che tra cinque anni violare una delle chiavi attualmente in uso divenga un compito relativamente semplice. Se così fosse, nel 2006 chiunque potrà produrre un documento provvisto di una perfetta ed ineccepibile firma digitale di Romolo Romani, datata 2001. E quindi i documenti sino a quel momento firmati con quella chiave cesseranno di essere affidabili, perché facilmente falsificabili. Questa è la ragione per cui i documenti perdono rilevanza giuridica con la scadenza della relativa chiave di firma digitale, siano essi autenticati o meno: anche la firma digitale del notaio scade, come tutte le altre. La ricevuta telematica con firma digitale di una trascrizione, gelosamente custodita in molteplici copie di sicurezza conservate magari in cassaforte, in meno di tre anni non significherà più nulla.

Panico? Non è proprio il caso. Un po' perché si è ben lungi dallo scrivere l'ultima parola in argomento. E poi perché, male che vada, per conservare la piena validità del documento è sufficiente poter dimostrare la sua anteriorità alla data di scadenza del certificato di firma. Ma come?

La via maestra (e l'unica che i veri informatici si degnino di prendere in considerazione) è l'apposizione della "marca temporale". Espressione tecnica che in realtà cela un'operazione molto semplice: il documento viene trasmesso ad un certificatore, il quale lo restituisce con una menzione provvista di data e firma digitale. Se un documento è stato firmato nel 2001 con una firma che scade il 31/12/2003, è sufficiente sottoporlo a marca temporale entro la fine del 2003 per protrarne la validità. Ma non all'infinito: la marca temporale non è altro che una firma digitale, e quindi scade a sua volta, riproponendo i medesimi problemi. La validazione temporale deve quindi essere compiuta periodicamente.

Certamente l'operazione potrà essere altamente automatizzata; inoltre non sarà necessario sottoporre a validazione l'intero documento, ma solo una sua "impronta digitale", riducendo la quantità di dati da trasmettere al certificatore e salvaguardando le esigenze di riservatezza. Ciò non toglie che laddove si abbia interesse a conservare l'efficacia probatoria di un documento, in capo al detentore incomba l'onere di un comportamento attivo provvisto di risvolti tecnologici non del tutto trascurabili. Prova in più (se mai ve ne fosse stato bisogno) dell'inderogabile necessità, per ciascuno di noi, di dotarsi di una cultura informatica che non si arresti ai primissimi rudimenti.

Ciò detto, non è escluso (anzi) che si possano adottare accorgimenti collaterali.

Solo un paio di esempi.

In una prima fase, con ogni probabilità, l'impiego della firma digitale sarà limitato alla trasmissione di atti e formalità da e verso la Pubblica Amministrazione. La conservazione informatica dei documenti da noi inviati, ad esempio, ai Registri Immobiliari, ricadrà sotto la responsabilità di questi ultimi; il notaio dovrà preoccuparsi invece dei documenti da lui ricevuti (la conferma dell'avvenuta registrazione e trascrizione, per cominciare). Nulla esclude che si organizzi il sistema in modo che una copia della ricevuta venga automaticamente fatta pervenire ad un soggetto tecnicamente ben attrezzato (Notartel, ad esempio) affinché ne assicuri la periodica validazione temporale e conservi il tutto presso i suoi archivi informatici, a disposizione del notaio per il caso di contestazione.

A costo poi di mandare definitivamente in bestia i veri informatici, azzardo un'eresia: in qualche caso potrebbe essere la cara vecchia carta a muovere in soccorso di questo bit dalla salute cagionevole. La marca temporale non ha altro scopo che dimostrare l'anteriorità di una certa firma digitale rispetto alla data di scadenza del relativo certificato. A me sembra che se la copia di una procura, trasmessa digitalmente dal notaio X al notaio Y, viene da quest'ultimo stampata ed allegata ad un atto, la data certa propria dell'atto medesimo assicura, una volta per sempre (siamo nel mondo cartaceo!), l'inattaccabilità dell'allegato.

Si potrebbe obiettare che la procura dell'esempio ha data certa di per sé, allegazione o non allegazione, ma così ragionando non si terrebbe probabilmente conto del fatto che qui si è di fronte ad un fenomeno del tutto nuovo: la giuridica scomparsa di un documento (la copia della procura), che prescinde completamente dalle caratteristiche intrinseche del documento stesso (in questo caso: dalla data certa che indubbiamente l'originale possiede). Può addirittura ipotizzarsi che l'originale di un documento informatico perisca e se ne conservi invece una copia presso un terzo che ne curi adeguatamente la validazione. Ammesso poi che la distinzione tra copia ed originale abbia ancora un senso compiuto, nel mondo digitale.

Il terreno, come si comprende, è ancora in buona parte da dissodare, e non ho la delirante pretesa di dispensare certezze. Su un punto (di metodo) vorrei però prendere posizione in modo risoluto. Quando da parte notarile vengono analizzate problematiche siffatte, la reazione da parte dei professionisti della firma digitale è sempre la medesima: raffiche di accuse furibonde, che dipingono i notai come i sabotatori delle sorti meravigliose e progressive del mondo telematico. La mia precisa sensazione è che simili contumelie debbano essere prontamente rinviate al mittente, e con gli interessi. Non vedo pericolo più grande, per un'ordinata e duratura introduzione della firma digitale nella nostra prassi, di un agire affrettato che pretenda di ignorare l'ovvio: i documenti relativi all'attività giuridica non bagatellare debbono offrire elevatissima sicurezza, avere una validità legale indiscutibile ed essere idonei ad essere conservati molto a lungo. Questi sono fatti, ed i fatti, se trascurati, hanno la pessima abitudine di vendicarsi.

Ugo Bechini notaio in Genova, membro della Commissione Informatica CNN