La nascita della firma digitale in Italia

di *Pierluigi Ridolfi*

Il prof. Romano Oneda, nell'invitarmi a questo Convegno, mi ha definito "*memoria storica della firma digitale*", appellativo che mi lusinga ma che dà anche un'idea del lungo periodo trascorso dalle prime riunioni sull'argomento.

Nello stendere una scaletta per questo intervento mi sono accorto che manca una storia dell'introduzione della firma digitale nel nostro Paese. Visto il tema del Convegno, "*Chi ha inventato il documento informatico?* ", ho pensato di ricostruire, almeno per sommi capi, le tappe principali del percorso che in quindici anni ha visto la firma digitale diffondersi in Italia come in nessun altro paese: i quattro milioni di dispositivi di forma digitale utilizzati oggi testimoniano un successo di gran lunga superiore a ogni previsione. Mi sembra anche che questa storia potrebbe costituire un argomento appropriato per delle originali tesi di laurea e di dottorato: è un'idea per l'uditorio che vedo composto in gran parte da giovani studiosi.

Torniamo allora indietro di quindici anni. Nel 1997, per iniziativa del Ministro della Funzione Pubblica Franco Bassanini, il Parlamento approva la legge 15 marzo 1997, n. 59 di riforma della pubblica amministrazione, nella quale, all'articolo 15, si legge: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti". È la prima volta che nel sistema giuridico italiano si parla di "documenti formati con strumenti informatici". Come previsto dalla legge, entro sei mesi, con il decreto del Presidente della Repubblica 10 novembre 1997, n. 513, viene emanato il relativo regolamento nel quale, all'articolo 1, si definisce non solo il "documento informatico" ma anche la "firma digitale" e, all'articolo 3, si dispone che con decreto del Presidente del Consiglio dei Ministri siano "fissate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici". Questo DPCM porta la data dell'8 febbraio 1999. Pochi mesi dopo l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA) pubblica la circolare per l'iscrizione nell'elenco dei certificatori. Si noti come l'intero pacchetto normativo – Legge, Regolamento, Regole tecniche, Circolare attuativa – veda la luce nell'arco di un paio d'anni.

Di firma digitale si parlava da tempo, soprattutto negli ambienti accademici americani, per l'originalità degli aspetti matematici che la caratterizzano, e in quelli militari, per il livello di segretezza che si potrebbe raggiungere nei messaggi, in relazione alla lunghezza delle chiavi adottate.
Per comprendere il perché di certe decisioni che furono prese allora dal legislatore e che ancora caratterizzano e vincolano l'impiego della firma stessa, occorre richiamare alcuni concetti alla base della tecnologia della firma.
Le formule matematiche sono note, ma i relativi programmi informatici sono difficili da realizzare perché operano su potenze binarie con esponenti molto grandi: sono un segreto industriale. Per garantire la segretezza collegata a questa tecnologia, il Governo americano nel 1990 vietò l'esportazione dei programmi di firma digitale per esponenti maggiori di 64 bit. La decisione suscitò reazioni negative in alcuni ambienti sostenitori della libertà d'espressione: Philip Zimmermann, che, oltre a essere un valente informatico, era un convinto assertore dei diritti umani, si oppose a questa decisione del Governo, organizzò molte manifestazioni di protesta, creò una

procedura completa di cifratura, adatta alla firma digitale e con chiavi molto lunghe, la inserì in Internet perché fosse liberamente scaricabile e usabile da chiunque. Questo atto gli costò l'arresto ma fu causa dell'immediata diffusione di questa tecnologia negli ambienti universitari (dove probabilmente non ce ne era affatto bisogno!).
Il tema di ricerca nuovissimo che ci si poneva era la lunghezza minima della chiave che rendesse la firma stessa inattaccabile da parte di malintenzionati: sarebbero bastati 128 bit? Oppure bisognava andare molto più in su, verso i 1024 bit? O addirittura i 2048? Dato che le chiavi sono date dal prodotto di due numeri primi "rompere" la segretezza della firma digitale richiede di risalire, data la chiave, ai due numeri primi che la compongono, il che si può fare solo per tentativi. Quando i numeri sono molto grandi, ciò è praticamente impossibile. Ma quanto "grandi" devono essere?
Si dimostra che con chiavi di 1024 bit non basterebbe l'età dell'universo.

Questa breve digressione matematica ha il solo scopo di giustificare il fatto che a quell'epoca - siamo a metà degli anni '90 - l'enfasi della firma digitale era tutta sulla sicurezza e sulla garanzia che la firma stessa non potesse essere alterata in modo doloso. Ciò ha influenzato in modo evidente il legislatore, che, come è ben noto, nella realtà è la sintesi delle personalità di più individui.

Lo sviluppo della firma digitale in Italia si deve a un gruppo di una decina di persone, guidati dall'AIPA, metà ingegneri metà giuristi. Essi stesero sia il DPR con il Regolamento sia il DPCM con le regole tecniche. Verso la fine del 1999 cominciarono ad arrivare le prime domande di iscrizioni e fu istituita un'apposita commissione di valutazione. Nel 2000 fu affrontato e risolto il problema dell'interoperabilità, si andò a regime e in Aipa venne creato un apposito ufficio, con a capo l'ing. Giovanni Manca. Accanto a tutti noi c'era sempre, e in prima linea, anche Manlio Cammarata, con la sua straordinaria rivista telematica, Interlex, che usciva un paio di volte al mese, con un britannico miscuglio di notizie e di vena polemica. Che aria si respirava? L'entusiasmo dei pionieri. Nessuno al mondo aveva ancora provato ad applicare la firma digitale nel campo amministrativo: si citava lo Stato dell'Utah, ma mancavano notizie precise.

Tornando alle norme, sia il DPR sia il DPCM risentono fortemente dell'atmosfera dell'epoca, molto influenzata, come già detto, dal problema della sicurezza. Il legislatore ebbe molto coraggio, mitigato però da una ampia dose di prudenza.

Porto qualche esempio.

I criteri previsti dal DPCM per i dispositivi di firma erano così ristretti che nessun dispositivo esistente in commercio li avrebbe mai superati. Erano stati preso a riferimento quelli stabiliti in generale da un ente internazionale sulla sicurezza denominato ITSEC, molto rigidi.. Quando arrivai a far parte del gruppo di lavoro la stesura del testo del DPCM era ormai completata. Feci presente che saremmo andati incontro a un disastro sostanziale e di immagine in quanto nessun operatore di firma avrebbe superato l'esame. Mi prendo il merito della soluzione. Agli originali 62 articoli del DPCM ne fu aggiunto in coda uno che recita così: "*Le disposizioni che richiedono verifiche secondo i criteri previsti da livelli di valutazione ITSEC non si applicano nei diciotto mesi successivi alla data di entrata in vigore delle presenti regole tecniche. Durante il periodo transitorio, il fornitore o il certificatore, secondo le rispettive competenze, devono tuttavia attestare, mediante autodichiarazione, la rispondenza dei dispositivi ai requisiti di sicurezza imposti dalle suddette disposizioni*". In pratica quest'articolo annullava in un colpo solo gli effetti potenziali di una decina di precedenti articoli.
L'idea dell'autodichiarazione – non stava alla commissione stabilire se fosse o meno veritiera – salvò la situazione, e fu reiterata numerose volte, di anno in anno, fino quasi ai giorni nostri. Da notare che, nell'esercizio pratico di gestione delle firme da parte di una ventina di certificatori, che ormai dura da dieci anni, mai ci furono manchevolezze attribuibili alla sicurezza dei dispositivi.

Un secondo esempio riguardò il terrore che si potesse dare a due diversi utenti la stessa chiave. A questo riguardo nell'articolo 28 si legge che: "*Prima di emettere il certificato il certificatore deve verificare che la chiave pubblica di cui si richiede la certificazione non sia stata certificata da uno dei certificatori iscritti nell'elenco*", operazione praticamente impossibile se non attraverso una banca dati monstrum contenente tutte le chiave emesse. Operazione che comunque è del tutto inutile, in quanto il sistema della firma digitale funziona benissimo anche se due o più utenti hanno la stessa chiave, *purché non lo sappiano*. Il fatto poi che due chiavi identiche siano emesse da due certificatori diversi non comporta nessun rischio applicativo, neanche remoto, in quanto i certificati sono diversi.

Purtroppo nelle stesura del DPCM fu fatto un errore concettuale che si trascina ancor oggi: infatti, proprio per presunte ragioni di sicurezza, fu introdotto l'articolo 60: "*La validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una o più marche temporali*". Non può essere così: un documento, cartaceo o informatico, firmato vale per sempre se la firma è stata posta in modo valido. Purtroppo quest'articolo dice il contrario e introduce il concetto, giuridicamente incoerente, che se il documento è informatico la firma digitale ha una validità limitata nel tempo e per essere rinnovata ha bisogno di una procedura di "rinfrescatura" attraverso il rinnovo della marca temporale. Che assurdità!
Purtroppo non c'è verso di far riformulare questa norma, che compare ancora nella bozza delle nuove regole tecniche in corso di emanazione, come richiesto dalla nuova versione del Codice dell'Amministrazione Digitale.

Un'altra stranezza, dovuta ai soliti motivi, sta nell'articolo 6, sulla generazione delle chiavi che, riassumendo, stabilisce che: "*1. La generazione della coppia di chiavi è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità della coppia generata. 2. Il sistema di generazione della coppia di chiavi comunque assicura l'utilizzo di algoritmi che consentano l'equiprobabilità di generazione di tutte le coppie possibili*". Requisiti del tutto inutili, perché, come già detto, in realtà non ha nessuna influenza il fatto che più persone abbiano la stessa chiave: importante è che abbiano certificati diversi, il che accade sempre.

Per motivi che non sono riuscito a capire, l'Italia non volle mandare formalmente a Bruxelles la bozza del DPCM per esame e approvazione, come stabilito dalle norme europee. Fui mandato invece io a presentarla, in modo informale e prima che comparisse sulla Gazzetta Ufficiale. L'occasione fu un mega-convegno organizzato dalla Comunità proprio sul tema della firma digitale e in particolare dell'interoperabilità. A rappresentare l'Italia c'ero io, da solo; tutti gli altri paesi avevano una delegazione di una ventina di persone, con a capo un Ambasciatore. Esposi il contenuto del nostro decreto. Mi fu detto che in alcuni punti non era in linea con lo schema di Direttiva sulle firme elettroniche che la Comunità stava elaborando: mi accorsi – ci accorgemmo – solo allora che su questa importantissima Direttiva in Italia non ne sapevamo niente. Tutta la ricca corrispondenza precedente era rimasta nei cassetti di qualche Ministero.

Nel dicembre di quello stesso anno, il 1999, uscì questa Direttiva, che ha un'impostazione molto diversa dalla nostra: l'ottica prevalente è quella del commercio elettronico, in un clima di libertà di mercato, mentre la nostra è tutta rivolta alla documentazione amministrativa. Sono menù diversi che è difficile servire allo stesso tavolo.

Ci fu un grosso lavorio per costruire un compromesso tra la nostra norma originaria e la Direttiva Europea e per inserirla nel nostro sistema giuridico. Si passò per varie fasi per approdare, in fine, nel Codice dell'Amministrazione digitale.

Non è possibile riassumere in poche righe quest'ultima parte della storia: mi limiterò a dire che fino alla penultima versione del Codice dell'Amministrazione digitale i tipi di firma elettronica erano tre: semplice, qualificata, digitale. Con il nuovo Codice si è aggiunto un quarto tipo di firma: quella avanzata.

Ma su questo argomento vi intratterrà l'ing. Giovanni Manca: l'avventura non è affatto finita.