V. Rizzo (a cura di), "Documento informatico, firma digitale e commercio elettronico"
Collana ITTIG-CNR, Serie "Studi e documenti", n. 2, Napoli, ESI, 2000, pp. 285-286

Intervento su:

Alcuni concetti relativi ai sistemi di firma digitale

MASSIMILIANO MINERVA

I sistemi di firma elettronica sono destinati gradatamente, ma inesorabilmente, a sostituirsi alle tecniche di firma tradizionali; non si tratta di una mia affermazione personale, ma lo dicono il mercato, l'evoluzione tecnologica e tanti atti normativi internazionali, comunitari e ora anche nazionali.

Sgombrato il campo da questa premessa generale, occorre fare una premessa di tipo terminologico: purtroppo molti dei termini utilizzati dal nostro legislatore, sia nel D.P.R. 513, che nel D.P.C.M., sono il frutto di una traduzione di termini anglosassoni.

Passiamo ora alla parte sostanziale del mio intervento.

La certificazione non è una certificazione amministrativa, ma tecnica, quindi la soluzione per il problema della certificazione sta proprio nel ritenerla appunto non un fenomeno amministrativo, bensì tecnico, cioè l'accertamento tecnologico della corrispondenza fra la chiave pubblica e il soggetto, per cui si tratta di un fenomeno di titolarità, consistente nell'attribuzione tecnologica di una sequenza di elementi informatici ad una chiave pubblica.

Non c'è, quindi, una certificazione dell'identità personale e questo potrebbe essere un problema e lo è senz'altro sotto il profilo della mancanza di un'identità personale certa dal punto di vista fisico.

La certificazione ci interessa, dunque, in quanto elemento tecnico, il certificato appunto, che si allega alla firma, elemento tecnico di una fattispecie tecnologica complessa, la firma digitale.

Questo significa che l'autorizzazione non è un'autorizzazione ad un'attività di tipo pubblicistico e, quindi, il sistema previsto dal nostro legislatore non andrebbe ricondotto ad un sistema di autorizzazione preventiva, come è stato fatto prima della direttiva, che ora impone di considerarla facoltativa.

Ha ragione Cardarelli quando sostiene che vi è una disarmonia da correggere, ma il sistema delle fonti è stato pensato quando ovviamente non esisteva quest'opzione in sede comunitaria.

Secondo problema, che desidero far notare, è quello della certificazione incrociata (*cross certification*) ed intendo sempre la certificazione della chiave pubblica.

A differenza ad esempio degli Stati Uniti, noi abbiamo disegnato un sistema di certificazione orizzontale, lasciando liberi i certificatori di scegliere tra due o più *standards* di fatto, identificati nel D.P.C.M. Ciò significa che ogni certificatore possiede la facoltà di scelta dell'algoritmo di decifratura tra i due indicati (RSA e DSA) e può scegliere il formato del certificato; conseguenza inevitabile è che se i certificatori, che sono soggetti privati, scelgono formati e criteri diversi tra loro, i sistemi non si parlano in assenza di accordi di certificazione.

Quindi il vero problema sarà far sì che i certificatori utilizzino gli stessi sistemi o stipulino accordi di certificazione incrociata, in modo che, come oggi si teme, la firma elettronica non finisca per valere in ambiti settoriali distinti: un certificatore, un àmbito settoriale, una firma elettronica. A questo fine sarà opportuno studiare delle soluzioni in proposito.

Concludo, infine, con una considerazione di gerarchia delle fonti, facendo notare che sicuramente esiste un problema a monte.

Nell'articolo 15 della legge n. 59 non abbiamo potuto decidere di utilizzare il sistema Legge di delega - decreto legislativo - regole tecniche, ma il sistema è diverso: Legge n. 59 del 1997 - D.P.R. ai sensi del comma 2 dell'art. 17 della legge 400-Regolamento, con tutte le relative conseguenze in termini di disapplicabilità e di impugnabilità, che sappiamo.

Il sistema è dunque strutturalmente debole e ciò va tenuto sempre presente, sforzandoci, a mio parere, per individuare le situazioni giuridiche e tecnologiche in grado di far sì che questo sistema, destinato a sostituire le tecniche di firma elettronica tradizionali, si realizzi compiutamente.