Dalla firma digitale alla firma elettronica qualificata

Firma informatica: Dalla firma digitale alla firma elettronica qualificata

Dott. Pasquale Lopriore
(p.lopriore@libero.it)

INDICE

1. Evoluzione normativa

Nell'ultimo decennio si è avviata una continua evoluzione nel campo del diritto delle tecnologie informatiche, partendo proprio dall'introduzione del concetto di documento informatico e della sua comparazione con quello cartaceo[1].

Se in ambito amministrativo si è riscontrata una timida presa di coscienza nei confronti delle nuove tecnologie con l'art. 22 della legge n. 241/1990; in ambito penale si è disciplinato direttamente il documento informatico con l'art. 491 bis, introdotto con la legge n. 547/1993, dando una sua prima definizione precisa *"qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli"*.

Questa definizione di documento informatico viene rimodellata con gli artt. 1 ss. del d.p.r. n. 513/1997, emanato in attuazione dell'art. 15 comma 2°, della legge n. 59/1997 (legge Bassanini-uno) secondo cui è tale *"la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*.

Il regolamento attuativo citato, non si limita a fissare la definizione di documento informatico ma va oltre, introduce in concetto di firma digitale definendola *"il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"*. Questo passo del legislatore del 1997 si può, senza dubbio, definire avanguardistico, poiché precede di gran lunga il legislatore europeo, che solo due anni dopo ha disciplinato questa materia.

In seguito, sono state apportate delle modifiche di carattere tecnico, per mettere in moto il meccanismo studiato per la firma digitale, con l'emanazione del D.P.C.M. del 08/02/1999, oltre alle varie circolare emanate dalla AIPA[2]. In quadro normativo italiano si completava con l'emanazione del T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, d.p.r. n. 445/2000.

Occorre subito evidenziare, che il legislatore italiano ha seguito una via ben diversa rispetto a quella seguita dal legislatore europeo, comportando non pochi problemi sotto il punto di vista del coordinamento tra le due legislazioni, colmato solo di recente con il D.Lgs. 7 aprile 2003 n. 137[3].

La normativa italiana, infatti, si inerpica su una regolamentazione rigida e dettagliata sia sotto l'aspetto della procedura informatica, che consente di apporre la firma digitale, sia per quanto riguarda i soggetti preposti alla sua realizzazione.

Già dalla definizione di firma digitale, precedentemente annunciata, si comprende il tenore della norma, infatti, afferma che solo con l'utilizzo di un sistema di crittografia a chiavi asimmetriche si può applicare la firma digitale su un documento, quindi, chiudendo ogni possibilità di utilizzazione di un'altra tecnologia che offre gli stessi risultati.

Di altro avviso è stato il legislatore europeo, che ha disposto un principio neutrale sulla validità delle firme digitali e promovendo la libera circolazione dei servizi di certificazione.

In particolare, sotto il primo aspetto la Direttiva non da un'unica nozione di firma digitale ma distingue tra firma elettronica semplice e firma elettronica avanzata, garantendo con quest'ultima oltre alla provenienza del documento anche l'integrità.

La naturale conseguenza di questa distinzione comporta il differente valore probatorio della firma elettronica in se.

Il legislatore italiano ha dovuto, di conseguenza, dare attuazione alla Direttiva disponendo una normativa aderente ai principi in essa esposti.

Con il D.Lgs. n. 10/2002, infatti, si disciplinano più tipi di firme informatiche dove quella digitale è una species rispetto al genus firma elettronica, invece, sotto un altro profilo il D.Lgs. n. 10 attesta l'istituzione del libero accesso al mercato dei certificatori.

Stante le novità apportate con questa norma, si apre un nuovo capitolo nella disciplina delle tecnologie atte a parificare e dare validità al documento elettronico rispetto al documento cartaceo.

In ultima analisi, questa evoluzione ha innescato il bisogno di un coordinamento con tutte le norme precedenti, come il d.p.r. n. 445/2000 che raccoglie tutto le norme in materia di firma digitale e documento elettronico.

A prendere atto di questo bisogno è stato il d.p.r. n. 137/2003, regolamento

recante disposizioni di coordinamento in materia di firma elettronica a norma dell'art. 13 del D.Lgs. n.10/2002.

Attualmente, per firma digitale si deve intendere come un *particolare tipo di firma elettronica_qualificata* basata su un sistema di coppia di chiavi asimmetriche, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

2. Procedimento per l'apposizione delle firma digitale

Occorre capire il funzionamento concreto della firma digitale, secondo il sistema scelto dal legislatore italiano, basato sulla utilizzazione di una coppia di chiavi asimmetriche, una privata e quindi segreta e l'altra pubblica ritrovabile negli appositi elenchi[4].

Questo sistema deve garantire due requisiti contemporaneamente:

- provenienza del documento firmato;
- segretezza del documento stesso.

Il primo requisito si ha quando il sottoscrittore appone la sua firma digitale sul documento e un soggetto qualsiasi poteva, consultando gli elenchi, risalire alla chiave pubblica e cosi decodificava il documento, ma appunto qualsiasi persona poteva conoscere il contenuto del documento anche se non poteva affermare che provenisse da un altro soggetto.

Con un altro sistema, invece, si può garantire solo la segretezza del documento questo quando il soggetto che sottoscrive il documento utilizza la chiave pubblica del soggetto destinatario, quindi solo quest'ultimo può decodificarlo utilizzando la sua corrispondente chiave privata.

I due requisiti, invece, sono garantiti con la combinazione delle due ipotesi

nel senso che il soggetto sottoscrittore deve prima cifrare il documento con la sua chiave privata, cosi garantendo l'autenticità, e una seconda volta con la chiave pubblica del destinatario, rendendo in questo modo il documento segreto[5].

Il soggetto destinatario dovrà, per leggere il documento, decodificare prima con la sua chiave privata e poi con la chiave pubblica del sottoscrittore.

In altre parole, per avere i due requisiti occorre utilizzare contemporaneamente la coppia di chiavi dei soggetti sia per codificare che per decodificare.

In questo sistema necessita anche di un sistema di compressione di file basato sulla funzione Hash, come disciplinato dall'art. 1 lett. c) dell'Allegato tecnico al d.p.c.m. 08/02/1999.

Il funzionamento della funzione Hash consiste nel comprimere i file scelti realizzando così delle impronte (o digest) corrispondenti che saranno tutte diverse tra di loro, perfino un semplice cambiamento della posizione di un carattere determina una impronta diversa.

In questo modo, il soggetto destinatario del documento deve, dopo la decodificazione con la propria chiave privata, confrontare l'impronta ricevuta con quella da egli generata. In concreto, tale sistema permette la non modifica del documento munito di firma digitale.

Schematicamente l'operazione di apposizione della firma digitale si risolve nei seguenti passaggi.

Operazione del soggetto sottoscrittore:

1. generazione dell'impronta;
2. creazione della firma digitale, apponendo la chiave privata all'impronta ricavata;

3. unione della firma digitale al documento.

Operazioni del soggetto destinatario:

1. separazione del documento dalla firma digitale;
2. creazione dell'impronta dal documento ricevuto;
3. utilizzo della chiave pubblica per decodificare;
4. confrontare le due impronte.

3. Il ruolo dei certificatori

Un tassello importante per completare il sistema delle firme digitali è costituito dai fornitori di servizi di certificazione (corrispondenti agli Certification Authority americani), non sono altro che soggetti estranei rispetto agli utilizzatori della firma digitale, ma devono garantire il funzionamento del meccanismo della firma digitale.

In particolare, i certificatori devono attestare che il soggetto detentore della chiave privata corrisponda alla relativa chiave pubblica, garantendo la sua identità. Altra funzione importante è attestare la validità del certificato mediante l'aggiornamento degli elenchi di dominio pubblico.

Queste funzioni sono racchiuse nella produzione del certificato della firma elettronica, costituito da un documento digitale che contiene il nominativo del titolare della firma e altre informazioni inerenti, come la durata della stessa; infine, questo certificato deve essere reso pubblico insieme alla chiave pubblica[6].

La figura del certificatore è stata anch'essa interessata alle modifiche apportate dalla direttiva europea dell'1999, di seguito recepita dal D.Lgs. n. 10/2002, introducendo il principio della libertà dei certificatori e varie forme di certificazione[7].

Significativa era la disciplina dei requisiti necessari che devono avere i certificatori privati, disposta nell'art. 8 del d.p.r. n. 513/97, la quale richiedeva, oltre all'inserimento in un apposito elenco pubblico, tenuto dall'AIPA e consultabile in via telematica, anche una forma societaria specifica quale la società per azioni, a capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria.

La norma richiedeva, sotto il punto di vista organizzativo interno, per i rappresentanti legali e i soggetti esposti all'amministrazione possiedano i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministratore, direzione e controllo presso le banche; invece, per il personale tecnico siano in grado di rispettare le norme del regolamento e le tecniche, nonché la qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

In conclusione, tutti i soggetti privati che vogliono occuparsi dell'attività di certificazione sono assoggettati ad un controllo preventivo sui requisiti richiesti.

Questo quadro, appena descritto, è stato stravolto dal D.Lgs. n. 10/2002 il quale dispone la libertà dell'attività dei certificatori abolendo una autorizzazione preventiva[8].

In questo modo, si introducono vari tipi di certificatori che possono rilasciare differenti tipi di certificati con differenti livelli di sicurezza (riconoscendo ai certificatori un accreditamento facoltativo dei requisiti di un livello più elevato); l'utente in base alle sue esigenza potrà scegliere il livello di sicurezza desiderato.

L'art. 2, comma 1, della norma citata, infatti, distingue tra certificati elettronici e qualificati, i primi sono definiti "*gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l' identità dei titolari stessi"* emessi dai certificatori accreditati e non. Per quanto riguarda i

certificati qualificati si devono intendere *"i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall' allegato II della medesima direttiva"* si richiedono, in altre parole, particolari requisiti sia per il certificato che per il soggetto che emittente.

4. Valenza probatoria

Un punto di forte interesse, per gli utilizzatori della firma elettronica, è rappresentato dall'efficacia probatoria di un documento informatico firmato elettronicamente[9].

Questo argomento è stato oggetto di discussione nella dottrina già prima dell'introduzione della firma digitale con il d.p.r. n. 513/97, infatti, ci sono state varie interpretazioni sull'ambito applicativo dell'art. 2712 c.c. per quanto riguarda i documenti informatici, sul punto, la sentenza della Corte di Cassazione Civile n. 11445/2001, ha sgombrato i dubbi emersi, equiparando, sotto il profilo probatorio, i documenti informatici privi di firma digitale alle rappresentazioni meccaniche di fatti o cose disciplinate dell'art. 2712 c.c. Di conseguenza, il documento informatico forma piena prova, nel caso in cui non viene disconosciuto, sotto il profilo della conformità ai fatti o alle cose in esso rappresentate, dal soggetto contro il quale è prodotto il documento informatico.

Per quanto riguarda i documenti informatici firmati elettronicamente, invece, l'efficacia probatoria è data dal tipo di firma utilizzata e varia proporzionalmente in base alla sicurezza tradibile dal meccanismo di firma utilizzato.

Per il documento informatico con firma elettronica *"c.d. leggera"*, seguendo il principio precedentemente esposto, l'efficacia probatoria sarà liberamente valutabile, in base alle caratteristiche oggettive di qualità e sicurezza, da parte del giudice nel corso del giudizio, come affermato nell'art. 10 del d.p.r. n. 445/2000, modif. dall'art. 6 del D.Lgs. n. 10/2002.

La stessa norma rimarca, per quanto riguarda le firme elettroniche *"c.d. pesanti"*, quanto già disposto dall'art. 5 del d.p.r. n. 513/1997, per i documenti sottoscritti con la firma digitale, disponendo la stessa efficacia della scrittura privata ai sensi dell'art. 2702 c.c. Pertanto, l'intervento del D.Lgs. n. 10/2002 si limita a coordinare con quanto disposto dalla direttiva 1999/93/CE, aggiungendo accanto alla firma digitale la firma elettronica avanzata; è interessante rilavare, invece, che il legislatore richiede che la firma deve essere basata su un certificato qualificato ed deve essere generata mediante un dispositivo per la creazione di una firma sicura. In altre parole, alla luce del D.Lgs. n. 137/2003, fa piena prova il documento con la firma elettronica qualificata e non con la generica firma elettronica avanzata, esigendo, di conseguenza, il livello massimo di sicurezza ricavabile.

1 Cft. M. Pappalardo, Il recepimento della direttiva: in difesa del legislatore, del 03/07/2003, pubblicato sul siti www.interlex.it.

2 Autorità per l'informatica nella pubblica amministrazione, ora sostituita dal Centro nazionale per l'informatica nella pubblica amministrazione CNIPA, secondo l'art. 176 del D.Lgs. 30 giugno 2003 n. 196.

3 Sulla tecnica legislativa da legislatori europei vedi, G.Finocchiaro, Firma digitale e firme elettroniche. Il quadro normativo italiano dopo il d.legisl. 10/2002, in Contratto e impresa 2002, 858 e ss.

4 Sul funzionamento della firma digitale in generale vedi, G. Finocchiaro, Documento informatico e firma digitale, in Contratto e impresa, 1998, 956; Zagami, La firma digitale e sicurezza giuridica, Cedam, 2000, 62 e ss.; G.-Ciacci, La firma digitale, Il Sole 24 ore, 1999, 47 e ss.; M. Pizzacalla, Firma digitale: le novità legislative e regolamenti, in Impresa c.i., n. 3 del 31 marzo 2001, 453 e ss.

5 Cft. G. Peruginelli, La firma digitale: aspetti normativi e procedure operative, in Ciberspazio e diritto 2003, vol. 4, n. 1, 15 e ss.

6 Sul procedimento di certificazione vedi, I.R.S. Pacifico, Firme elettroniche come sistema di sottoscrizione dei documenti. Storia e prospettive, in Codici e Leggi d'Italia, De Agostani Professionale n.6/2003.

7 Cft. G. Nasi, Le ragioni dei certificatori accreditati "Relazione introduttiva del presidente di Assocertificatori al convegno Omat del 15/11/2002, pubblicato sul sito www.interlex.it .

8 In attuazione all'art. 3 comma 1 della Direttiva 1999/93/CE.

9 Cft. P. Russo, Firma digitale, forma scritta e requisiti formali, del 10/07/2003, pubblicato sul siti **www.intrelex.it** .