

Chiavi biometriche (Art. 1, lett. g, D.P.R. n. 513 del 1997)

ENRICO MACCARONE¹

In tema di firma digitale e documento informatico è singolare osservare come il mondo del diritto si sia attivato per disciplinare un fenomeno prima del suo nascere o, quanto meno, prima del suo diffondersi, e non - come ordinariamente avviene - per regolamentare un fenomeno o un istituto già consolidato nella pratica.

Non è logicamente possibile regolamentare una materia dai forti riferimenti tecnologici se non dopo avere operato precise scelte di campo, più o meno necessitate, all'interno dello scenario tecnologico di riferimento.

Nel caso del D.P.R. n. 513 del 1997 tali scelte sono state relativamente semplici per ciò che riguarda lo *standard* di generazione della firma digitale, essendosi già da tempo affermato in campo internazionale lo *standard* derivante dalle applicazioni delle chiavi asimmetriche di cifratura; meno semplici, e ne vedremo i motivi, le scelte relative all'infrastruttura di firma (la cosiddetta PKI - *Public Key Infrastructure*) ed alla regolamentazione degli enti preposti all'attività di certificazione.

Il metodo migliore per affrontare le tematiche che ci interessano, e più in particolare le tematiche collegate alle tecnologie di firma digitale a chiave pubblica, è indubbiamente quello di elencare in via preventiva - anche se per sommi capi - tutti i passaggi necessari per una corretta e valida utilizzazione del sistema.

Tali passaggi possono essere così semplificati:

1)- *fase preparatoria*:

- acquisizione di un *software* per la generazione della coppia di chiavi;
- generazione della coppia di chiavi;
- individuazione, per sua natura casuale, della chiave pubblica e della chiave privata;

¹ emaccarone@notariato.it

- **secretazione e conservazione della chiave privata su adeguato e sicuro supporto;**
- **invio della chiave pubblica al certificatore;**
- **ottenimento del certificato e sua archiviazione;**
- **pubblicazione del certificato presso il certificatore.**

II)- *fase gestionale*:

- **mantenimento in vita di tutti i presupposti soggettivi ed oggettivi per la validità del certificato;**
- *idem*, per mantenere l'inviolabilità delle chiavi personali.

III)- *utilizzazione*:

- **formazione del documento informatico;**
- **procedura di *hashing* e generazione firma digitale;**
- **apposizione marca temporale;**
- **conservazione, invio e archiviazione del documento informatico;**
- **gestione dell'archivio dei documenti.**

Il processo così definito rispecchia sia logicamente sia strutturalmente l'impianto del D.P.R. n. 513 del 1997 e, in particolare, la sequenza delle definizioni enunciate in seno al suo art. 1, una sequenza la cui logica viene apparentemente interrotta dalla definizione di "chiave biometrica" riportata al punto 1.g).

Ma a ben guardare tale collocazione non è frutto del caso, bensì di una precisa scelta strategica che vale la pena di approfondire, tesa ad evitare l'equivoco (dimostratosi abbastanza frequente) di ritenere sufficiente l'utilizzazione delle sole chiavi biometriche per lo sblocco delle chiavi di firma e la conseguente generazione di firme digitali. Un equivoco evidenziatosi sia durante i lavori preparatori al D.P.R. n. 513 del 1997, sia durante lo svolgimento dei numerosi convegni che nel corso degli ultimi due anni si sono svolti in più sedi sullo stesso D.P.R., e cioè l'equivoco di ritenere che l'apposizione della firma digitale possa esser fatta utilizzando come chiave di sblocco la sola impronta biometrica o, peggio ancora, utilizzando quale chiave di cifratura la "stringa" fornita dalla chiave biometrica.

Il processo di generazione della firma digitale è ovviamente collegato ad un'espressione di volontà del sottoscrittore e trova il proprio momento culminante e giuridicamente rilevante nella conferma di voler sottoscrivere, conferma fornita allo strumento informatico attraverso l'immissione di una serie di informazioni: tipicamente dalla digitazione di una *password* e, ove previsto, dall'immissione di ulteriori informazioni o di una o più chiavi biometriche.

L'impianto del D.P.R. n. 513 del 1997 e delle Regole Tecniche ad esso afferenti escludono di fatto che in generale tale processo possa dipendere esclusivamente dall'immissione di una o più chiavi biometriche, e ciò non tanto per motivazioni tecniche (di fatto inesistenti) quanto per precisi motivi giuridici strettamente collegati al "consenso" ed ai modi di formazione di esso.

La scienza ha nel tempo individuato almeno quattro elementi, tutti singolarmente individualizzanti, utili per distinguere un individuo da un altro:

- il "soma", corrispondente alla contemporanea rilevazione dei tratti del volto e della distribuzione del calore sullo stesso;
- l'impronta della retina;
- l'impronta digitale;
- l'impronta vocale.

Il primo ed il secondo sono ad oggi gli elementi di maggiore affidabilità; minore affidabilità viene riconosciuta al terzo ed al quarto, poiché (anche se raramente) replicabili o duplicabili in natura, nel senso che uno di tali elementi può essere presente contemporaneamente in più soggetti.

Rilevare il "soma" di un soggetto è operazione complessa, che ad oggi può essere svolta solo utilizzando tecnologie ad alto costo.

Ben più semplice ed economica è l'operazione di rilevamento delle altre tre impronte, oggi resa possibile da apparecchiature e programmi relativamente di basso costo, addirittura capaci (per il rilevamento dell'impronta digitale e della retina) di rilevare se la fonte dell'impronta è viva, se al suo interno vi sono circolazione sanguigna e conseguente calore.

Un'impronta - qualunque essa sia - viene rilevata in modo meccanico, nel senso che il soggetto da identificare non deve compiere alcuna particolare attività se non quella di poggiare un dito su un apparecchio, o guardare un punto fisso, o emettere un suono vocale.

Ma quale consenso può ragionevolmente farsi derivare dal guardare un punto fisso o compiere un'altra delle attività meccaniche ora dette? Certamente nessuno.

Ma vi è di più.

Se esaminiamo da vicino il modo di riconoscimento di una chiave biometrica, ci rendiamo subito conto del fatto che per consentire le necessarie elaborazioni, e quindi per la sua stessa esistenza, essa ha necessità di venire memorizzata anche temporaneamente su un qualsiasi supporto informatico: una volta rilevata, l'impronta viene collazionata con altra impronta precedentemente acquisita e solo in caso di raffronto positivo avviene il riconoscimento, la conferma di avvio del processo richiesto.

Il dovere archiviare un'impronta di riferimento - anche se per millisecondi - all'interno di un qualsiasi sistema informativo la rende per ciò stesso insicura, poiché si tratta pur sempre di informazione per sua natura duplicabile (non ha importanza se con tecniche semplici o sofisticate) e quindi in grado di annullare sul nascere il mantenimento del segreto collegato alla conservazione ed all'uso della chiave privata.

Peggio ancora se la rappresentazione informatica di tale impronta viene archiviata all'interno di un *database*.

Non è quindi un caso se nel D.P.R. n. 513 del 1997, parlando di chiavi biometriche, si faccia esclusivo riferimento a meccanismi di sicurezza ed in particolare a metodi di verifica dell'identità, ben stando attenti a non cadere nel tranello della genericità e ad evitare che dall'uso di chiavi biometriche possa farsi discendere una qualsiasi manifestazione di volontà.

Tutto ciò non esclude, però, che delle chiavi biometriche possa farsi uso per attivare processi serializzati o ripetitivi di generazione della firma digitale (es. la sottoscrizione di un alto numero di mandati di pagamento, o di lettere circolari): in tal senso «... si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del sottoscrittore» e sempre a condizio-

ne che «... prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all'identificazione del titolare» (art. 10 Regole Tecniche).

In conclusione: la firma digitale viene generata scatenando un processo che, utilizzando la chiave privata del titolare, conservata all'interno di un dispositivo di firma, rende disponibile tale chiave soltanto dopo avere identificato il titolare (anche a mezzo di chiave biometrica, nei limiti suddetti) e verificato la sua volontà di sottoscrivere (non verificabile, per i motivi suddetti e fatte salve le eccezioni ex art. 10 Regole Tecniche, attraverso la semplice immissione di una chiave biometrica)

Di tutto ciò, infine, abbiamo conferma diretta dalla lettura delle regole tecniche dettate con D.P.C.M. 8 febbraio 1999, che all'art. 8 dispongono la conservazione delle «... informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave», ed al successivo art. 10 ribadiscono la necessaria riconducibilità della sottoscrizione ad un'espressa manifestazione di volontà del sottoscrittore stesso.

Che la rilevazione di una chiave biometrica non possa essere considerata espressione di volontà è stato già sottolineato; a norma del richiamato art. 10 delle regole tecniche essa può invece essere considerata come ottima metodica per procedere all'identificazione del titolare (art. 10, comma 4), come strumento cioè di sicurezza così come descritto dall'art. 1, lett. g), D.P.R. n. 513 del 1997.

È appena il caso di sottolineare, per ultimo, che i dati biometrici "camminano" con il loro "titolare", vengono da esso portati e non conservati. Ammetterne la possibilità di separazione dal titolare e quindi la conservabilità porterebbe all'assurda conseguenza di una macabra ed impossibile previsione legislativa: quando non utilizzato, il dito (o la retina, o altro) va staccato dal corpo del titolare e conservato in luogo sicuro.