forze civili

ANNO IV **NUMERO 5/6** - SETTEMBRE-DICEMBRE '99

DIALOGO E CULTURA PER LA LEGALITÀ

Spedizione in abbonamento postale comma 27 dell'art. 2 legge 28 dicembre 1995 n. 549 Filiale P.T. Viterbo - L. 5.000 - Contiene I.R.

Sicurezza: il 2000 delle incertezze

Balistica. Gli effetti del munizionamento spezzato

ORGANO UFFICIALE DELL'ASSOCIAZIONE NAZIONALE FUNZIONARI DI POLIZIA

FIRMA DIGITALE: IL FUTURO È GIÀ ARRIVATO?

Esigenze di segretezza e crittografia

"Segreti, codici, crittografia ..." sembra di parlare di un film di spionaggio, in realtà si tratta dei concetti che stanno alla base di un nuovo istituto giuridico che in un "futuro" sempre più "presente" costituirà la regola per l'effettuazione di ogni transazione privata e di qualsiasi rapporto con una Pubblica Amministrazione, si spera, sempre più informatizzata.

Si tratta della c.d. "firma digitale" vale a dire di quella che il D.P.R. 10/11/97, n. 513, definisce in modo più appropriato come: "il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore, tramite la chiave privata, ed 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". Attualmente essa è il più sofisticato e sicuro sistema per assicurare l'integrità e la provenienza dei documenti informatici, sostituendo quella che nei documenti tradizionali è la firma autografa.

L'esigenza della regolamentazione della "firma digitale" è diventata di tutta evidenza, oltre che per motivi di maggior sicurezza rispetto alla firma autografa, anche in seguito allo sviluppo di "internet" che ha introdotto il concetto di commercio elettronico e delle "reti telematiche" di cui, secondo le tendenze più recenti, dovrebbe servirsi la Pubblica Amministrazione per rendere più veloci ed efficienti i propri servizi.

Ciò ha reso indispensabile, però, la protezione del flusso di informazioni che giornalmente circola per via telematica, per evitare che chiunque, anche non autorizzato, possa accedervi con facilità. Per far ciò si è dovuto attualizzare il vecchio concetto di crittografia da sempre utilizzata ma che, prima dell'era del computer, si basava sulla tecnica della "sostituzione" (delle lettere alfabetiche con altre lettere o segni di fantasia), o sul meccanismo della "permutazione", che si risolve in uno scambio di lettere tra loro.

Un esempio del primo metodo è quello della sostituzione di ogni singola lettera con quella che la segue nell'alfabeto, perciò il termine FIRMA diventerebbe GLSNB; un esempio dell'uso della tecnica della permutazione è invece quel che tutti noi abbiamo più volte visto nei settimanali di enigmistica e cioè "l'anagramma a chiave" dove le lettere vengono scambiate di posto in funzione di una regola ben precisa, per esempio scambiando le lettere pari con quelle dispari (questa sarebbe la chiave): il termine FIRMA diventerebbe IFMRA.

Oggi, i moderni computer consentono di integrare fra loro entrambi i metodi mediante algoritmi che permettono un numero di combinazioni quasi infinito (il DES, Digital En-

cryption Standard, – che è uno dei metodi più utilizzati fino a poco tempo fa, in quanto ritenuto tra i più sicuri – consente qualcosa come 72.000.000.000.000.000, settantaduemilioni di miliardi, di combinazioni).
La configurazione mista consente altissimi livelli di sicurezza ma ha lo stesso grave inconveniente dei sistemi meno recenti sopra descritti e cioè quello di essere basata su un'unica chiave che deve essere conosciuta da entrambe le parti, cosa che, nella globalizzazione del sistema costituisce un limite di tutta evidenza.
Per superare tale inconveniente fu "inventato" da alcuni matematici una tecnica nuova detta a doppia chiave asimmetrica, che consiste in un algoritmo che utilizza due chiavi di decrittazione, una pubblica nota a tutti, ed una privata, segreta e nota solo al destinatario.
Attraverso la prima chiave (quella pubblica) è possibile a tutti codificare i propri dati, mentre, solo attraverso la chiave privata, è possibile la loro decodifica.

La "firma digitale": evoluzione normativa

La disciplina della "firma digitale" consiste in un'evoluzione del sistema sopra descritto e prevede l'utilizzo combinato di hardware e software, attraverso il quale vengono depositati i dati personali dell'utente, generandone la firma elettronica e custodendone la relativa chiave privata.
Un'applicazione "primitiva" del principio è quella, da tempo operante, del Bancomat, dove la banca è titolare di una chiave pubblica liberamente fruibile che combinata elettronicamente con quella privata conosciuta solo dal titolare (il codice pin) consente di prelevare contante dagli sportelli appositamente predisposti dalle banche.

Come di consueto solo dopo parecchi anni dalla diffusione dell'informatica, anche a fini commerciali e pubblici il Legislatore ha "intuito" l'importanza di una regolamentazione dei sistemi per garantire la provenienza e l'autenticità del documento informatico.
"L'intuizione" l'ha avuta il legislatore del 1993 che, nella foga delle iniziative volte a "scardinare" il sistema amministrativo fondato sulla burocratizzazione della P.A., ha inserito nel decreto Legislativo 12/02/93, n° 39, il concetto di "integrale informatizzazione della P.A." disciplinando le modalità con cui la P.A. avrebbe dovuto intraprendere la progettazione, lo sviluppo e la gestione di sistemi informativi automatizzati.
Lo scopo era quello di ottenere "il miglioramento dei servizi, la trasparenza dell'azione amministrativa, il potenziamento dei supporti conoscitivi per le decisioni pubbliche ed il contenimento dei costi dell'azione amministrativa".
A tal fine venne lanciata l'idea di una "rete unitaria della Pubblica Amministrazione"; coordinata e gestita dall'AIPA (Autorità per l'Informatica nella P.A.) mediante "l'interconnessione telematica delle reti di ciascuna Amministrazione"; ciò, peraltro, avrebbe evitato lunghi ed inutili scambi cartacei di informazioni tra Amministrazioni.
Tutti questi principi sarebbero però rimasti al livello di mere enunciazioni teoriche, se la prima tra le cd. "leggi Bassanini" (n° 59/1997) non avesse dato un'improvvisa accelerazione al progetto con l'articolo 15 che dispone che "gli atti, dati e documenti formati dalla P.A. e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme nonché la loro archiviazione e trasmissione con mezzi informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità ...sono stabiliti ... con specifici regolamenti...".
Tale enunciazione di principio contiene in sé elementi rivoluzionari in quanto supera gli ostacoli normativi in base ai quali per dare rilievo giuridico agli atti amministrativi informatici era necessario che gli stessi venissero "riversati su carta" in modo da consentire la sottoscrizione autografa su originale e le timbrature varie che ne certificassero la provenienza.
Con il citato articolo 15, viceversa, si dà rilievo all'attività giuridica posta in essere esclusivamente attraverso canali telematici in assenza cioè di qualsiasi supporto cartaceo.
Il primo dei decreti attuativi previsti dalla disposizione in esame è stato, in ordine di tempo, quello relativo ai "criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15/03/1997, n° 59" sotto il profilo sia pubblicistico che privatistico (D.P.R. 10/11/97, n° 513).
Il secondo, e più complesso, provvedimento è stato quello relativo alle "regole tecniche per la formazione, la trasmissione, la conservazione la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi..." (D.P.C.M. 08/02/1999).
Siamo, dunque, già nel futuro?
Per poterlo dire con certezza occorre analizzare entrambi i suddetti decreti sia dal lato tecnico che da quello, maggiormente rilevante ai nostri fini, giuridico, ma questo è tutto un altro discorso ...!

Dr. Giuseppe Motta
Funzionario amministrativo
del Ministero della Difesa
(per Ufficio Studi
A.N.F.P. Regione Sicilia)