

## **Le nuove disposizioni in materia di firme elettroniche**

di Carlo Notarmuzi

E' in atto in Italia, a partire dal 1997, un percorso normativo diretto ad attribuire alla firma elettronica e digitale piena valenza giuridica, tale da produrre effetti giuridici equivalenti a quelli conseguibili mediante la firma autografa apposta su supporto cartaceo.

Questo percorso ha attraversato due diverse fasi.

In un primo momento, nel 1997, l'Italia, ponendosi all'avanguardia rispetto a tutti gli altri paesi europei, ha introdotto la disciplina del documento informatico e della firma digitale<sup>1</sup>.

La materia, oggetto di un intervento di delegificazione, è stata inizialmente regolata con il decreto del Presidente della Repubblica. 10 novembre 1997, n. 513, successivamente confluito nel Testo unico sulla documentazione amministrativa 28 dicembre 2000, n. 445, adottato ai sensi dell'art. 7 della legge n. 50 del 1999. Il quadro normativo è stato poi completato con la definizione delle relative regole tecniche, approvate con il decreto del Presidente del Consiglio dei ministri 8 febbraio 1999.

La seconda fase, attualmente in corso, è caratterizzata dall'opera di revisione del sistema normativo italiano relativo alla firma digitale, reso necessario dal sopravvenuto intervento sulla materia da parte dell'Unione europea, che nel 1999 ha approvato la direttiva n. 93, il cui recepimento è stato disposto dalla legge 29 dicembre 2000, n. 442, (legge comunitaria 2001)<sup>2</sup>.

---

<sup>1</sup> Per alcuni spunti sul documento informatico A. Masucci, *Il documento amministrativo informatico*, in *La documentazione amministrativa*, (a cura di G. Arena), Rimini, 2001; e per la giurisprudenza si veda Cassazione, sezione quinta penale, 14 marzo-12 maggio 2003, n. 20723, secondo la quale le fattispecie di falso materiale e ideologico, previste dal codice penale, si configurano anche quando la falsificazione sia avvenuta a mezzo di un supporto informatico.

<sup>2</sup> E. Granelli, *La firma digitale europea*, in *Giornale di diritto amministrativo*, n. 7/2002, p. 739, il quale evidenzia due diverse soluzioni adottate in ambito europeo. Da un lato Italia e Germania, che hanno adottato maggiormente sicuri, da un altro lato paesi anglosassoni, che hanno adottato soluzioni più agili e meno costose, ma anche meno sicure.

## **Il quadro normativo: testo unico decreto legislativo e decreto del Presidente del consiglio dei Ministri**

Il quadro normativo che si delinea con l'entrata in vigore del decreto del Presidente della Repubblica 7 aprile 2003, n. 137, non è dei più lineari tra quelli che si presentano all'operatore<sup>3</sup>.

Il testo unico n. 445/2000 aveva raccolto in un'unica fonte tutte le norme in materia di firma digitale fino ad allora emanate. Il recepimento della direttiva 1999/93/CE ha comportato la necessità di emanare il decreto legislativo 23 gennaio 2002, n. 10 per modificare le norme di rango legislativo ed il decreto del Presidente della Repubblica, che qui si commenta per modificare le norme di rango regolamentare.

Purtroppo il d.lgs. n. 10/2002 non ha rispettato quanto previsto dall'articolo 7, comma 6, della legge n. 50/1999 in materia di testi unici, che prevedeva l'inserimento delle modifiche, successivamente intervenute, direttamente nel testo unico mediante la tecnica della novella: la norma delegata ha, invece, innovato l'ordinamento in una duplice direzione, da un lato mediante modifiche del testo unico, da altro lato, introducendo autonomamente norme nell'ordinamento.

Conseguentemente nonostante l'esistenza di un testo unico alcune norme relative alle firme elettroniche sono contenute anche al di fuori di esso e più precisamente nel decreto legislativo n. 10 del 2002.

Non si può inoltre trascurare il decreto del Presidente del Consiglio dei ministri, attualmente in corso di emanazione, che contiene le regole tecniche sulla firma elettronica; in questo caso trattandosi di un provvedimento amministrativo non poteva che trovare autonoma collocazione.

## **Che cos'è la firma digitale**

La definizione relativa alla firma digitale era già contenuta nel testo unico in materia di documentazione amministrativa, ma è stata modificata al fine di adeguarla alla mutata tecnologia.

L'articolo 1, comma 1, lettera n) del d.p.r. n. 445/2000, come modificata dal d.p.r. n. 137/2003, definisce la firma digitale, "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, 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".

---

<sup>3</sup> Per un commento al d.p.r. 7 aprile 2003, n. 137, si veda anche G. Cammarota, *La nuova regolamentazione della sottoscrizione informatica*, in *Giornale di diritto amministrativo*, n. 5/2003, 451.

Volendo trasferire questa definizione nella nostra realtà quotidiana, possiamo partire dallo strumento che si utilizza per apporre una firma digitale: si tratta di una smart-card cioè di una tessera del tutto simile ad un bancomat o ad una carta di credito, all'interno della quale è custodito un microchip. La smart-card deve essere inserita in un piccolo lettore che si applica a qualsiasi personal computer. Utilizzando un codice numerico (codice PIN) analogo a quello utilizzato per i bancomat, è possibile sottoscrivere il documento informatico.

E' opportuno precisare che tale sottoscrizione non ha nulla a che vedere con la nostra firma apposta con la penna. La presenza della firma digitale è riconoscibile solo dall'estensione del file identificabile come "p7m" e, in alcuni casi, dalla presenza di un'icona che identifica il soggetto che ha rilasciato la firma; si tratta di dati che certamente non ci aiutano ad identificare il soggetto che ha sottoscritto il documento. Poiché la firma elettronica non garantisce solo l'autenticità della firma ma anche l'integrità del documento, il file p7m, rappresenta anche una sorta di busta elettronica. Aprendo il file, grazie alla chiave pubblica contenuta nella firma, è possibile leggere sia il documento, sia il certificato elettronico di firma che ci fornisce le informazioni necessarie ad identificare chi ha sottoscritto il documento: il nome la data di rilascio, la data di scadenza ecc. Queste in estrema sintesi le caratteristiche tecnologiche della firma digitale.

## **I contenuti del provvedimento**

Attraverso il nuovo regolamento si delineano nuove tipologie di firma elettronica, in aggiunta alla firma digitale già in uso nel nostro paese, in adesione ai precetti forniti dalla Commissione europea.

Esaminando l'articolo 1 del regolamento, relativo alle definizioni, si identificano quattro tipi di firma: la firma elettronica (lettera cc), la firma elettronica avanzata (lettera dd) la firma elettronica qualificata (lettera ee) e la firma digitale (lettera n).

L'Unione europea ha richiesto che il recepimento della direttiva avvenisse mediante una normativa neutrale alla tecnologia, e cioè tale da consentire l'evoluzione tecnologica indipendentemente dalla scelta normativa operata; analogamente l'applicazione dell'informatica al diritto deve avvenire senza alterare gli istituti giuridici.

L'esistenza di quattro tipi di tipi di firma sembrerebbe non confermare tale scelta, poiché il nostro ordinamento riconosce solo due tipi di firma: la firma autografa e la firma autenticata. Occorre pertanto cercare di analizzare le varie definizioni di firma elettronica, al fine di rapportarle alla firma autografa apposta su un documento cartaceo.

La firma elettronica costituisce una nozione molto ampia che mal si concilia con la nozione di firma comunemente nota intesa come “il nome sottoscritto a titolo di convalida, attestazione o adesione personale”<sup>4</sup>, che costituisce “un dato somatico e personale, che risulta in un segno diverso per ogni soggetto che l’appone”<sup>5</sup>.

Per firma elettronica si intende qualsiasi forma di identificazione *on line* dell’utente, o per usare la terminologia adottata dal legislatore, si intende l’autenticazione informatica del soggetto. Come accade ad esempio per l’uso del bancomat, attraverso il codice numerico c.d. PIN l’utente si identifica per poter compiere determinate operazioni; oppure con le modalità attraverso le quali ci si può identificare nella rete telematica, attraverso *username* e *password*. Queste sono comunemente definite come “firme 5.2” dalla norma della direttiva comunitaria che le disciplina. Tuttavia non si tratta di firme secondo l’accezione comune del termine come sopra descritta, ma si tratta solamente di uno strumento di sicurezza di autenticazione in rete. In questa forma di identificazione manca la caratteristica dell’univocità, cioè la possibilità di ricondurre tale firma ad un determinato soggetto e solamente a quello.

Tale caratteristica è presente, invece, nella “firma elettronica avanzata” definita come “la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce, in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati” - art. 1, comma 1, lett. dd) del d.p.r. n. 445/2000 -.

Correttamente la firma elettronica avanzata è stata definita come un “contenitore vuoto”<sup>6</sup>, cioè una categoria di possibili firme, che, tuttavia, al momento, la tecnologia non è in grado di riempire con tipologie reali ed utilizzabili. Possiamo prevedere che in futuro nell’ambito di firme elettroniche avanzate verremo a ricomprendere forme di firma quali la sottoscrizione mediante il riconoscimento dell’iride, ma al momento si tratta di una potenzialità non compiutamente realizzata.

Sia la firma elettronica *tout court* che la firma elettronica avanzata sono riconducibili quanto disposto dall’articolo 10, comma 2 del d.p.r. n. 445/2000, il quale stabilisce che il documento firmato elettronicamente “è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza”. Non si tratta però di una firma assimilabile alla firma autografa.

Caratteristiche oggettive di qualità e sicurezza sono rinvenibili nella firma “firma elettronica qualificata”. Ad essa, infatti, sono riconducibili oltre

---

<sup>4</sup> Devoto Oli

<sup>5</sup> R. Zagami, *Le firme elettroniche*, p. 20, 2003

<sup>6</sup> De Giovanni Caserta

alle caratteristiche che rendono tale una firma prodotta elettronicamente, quali la riconducibilità univoca della firma al suo sottoscrittore, la non alterabilità o modificabilità della firma medesima e quindi l'uso di una tecnologia affidabile, le caratteristiche di qualità e sicurezza proprie dei servizi di certificazione "qualificati".

Alle caratteristiche di univocità ed autenticità si aggiunge un ulteriore elemento di sicurezza e cioè l'intervento di un soggetto terzo che certifica la corrispondenza della firma al suo titolare.

In sintesi gli elementi che caratterizzano le tipologie di firma sono tre: chi firma, con quale tecnologia firma e chi certifica le caratteristiche della firma. Su questi tre pilastri è stato costruito il regolamento: introdurre nell'ordinamento una firma che abbia tutti e tre questi requisiti.

Il primo aspetto, come detto è rappresentato da "una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati", caratteristica questa presente nella firma elettronica avanzata.

Il secondo aspetto, relativo alla non alterabilità o modificabilità riguarda la tecnologia usata. In Italia la tecnologia applicata è, come detto, quella digitale.

Il tema della tecnologia utilizzata per firmare elettronicamente risale al decreto del Presidente della Repubblica 10 novembre 1997, del 1997, che ha introdotto nel nostro ordinamento la firma digitale. L'etimologia di tale nozione deriva dall'espressione inglese *digit*, cioè cifra. Infatti la firma digitale non è altro che un numero (molto grande nell'ordine di qualche centinaia di cifre, ma pur sempre un numero). Si tratta di una semplificazione estrema della tecnologia della firma che si basa su un sistema di chiavi crittografiche cioè la tecnologia attraverso la quale è possibile trasformare un testo o dato cifrato in un testo o dato leggibile (c.d. in chiaro). Tale tecnologia si basa su una chiave privata in possesso del titolare che consente di apporre la firma "cifrata" ed una pubblica, che allegata a quella privata consente di "leggere", la firma.

Questa tecnologia, è quella universalmente adottata in Europa, ma ciò ha paradossalmente creato delle difficoltà al legislatore italiano, in quanto, quando nel 1999 l'Unione europea ha adottato la direttiva sulle firme elettroniche, ha voluto dettare una disciplina non solo connessa alla firma digitale, ma che potesse prevedere qualsiasi tipologia firma che si avvallesse della tecnologia elettronica, quali ad esempio l'identificazione mediante l'impronta digitale. In tal modo il nostro ordinamento ha dovuto adeguare il proprio sistema normativo alle disposizioni comunitarie, non corrispondenti alla tecnologia avanzata applicata in Italia e basate su una nozione astratta di

firma elettronica. Questo perché il principio affermato in ambito comunitario si fonda, come detto, sulla neutralità della norma giuridica rispetto alla tecnologia, con ciò intendendo che le disposizioni normative dovessero essere tali da consentire l'applicazione di qualsiasi soluzione tecnologica. Tale costruzione di pregevole fattura, costituisce un'utile indicazione per tutti quei paesi nei quali la firma elettronica non ha ancora trovato applicazione; nel nostro paese tale assunto ha presentato notevoli difficoltà applicative, in quanto si è dovuto innestare il sistema tecnico-giuridico esistente, basato sulla firma digitale, su un sistema giuridico neutrale a qualsiasi soluzione tecnologica.

Ci si è così trovati di fronte ad uno scenario normativo che da un lato prevedeva una tipologia ampia di firma ma astratta, quale è la firma elettronica, e da un altro lato disciplinava una tipologia concreta, reale ed applicabile di firma elettronica: la firma digitale.

Per poter coniugare tali esigenze la rubrica della sezione V del capo II del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, intitolata "firma digitale" è stata sostituita con la rubrica "firma elettroniche", proprio al fine di poter prevedere diverse tipologie di firme elettroniche tra le quali anche quelle digitali. Alcune norme, però disciplinano solo la firma digitale, poiché, come detto, al momento, è l'unico tipo di firma concretamente utilizzabile. Tale impostazione è confermata dai contenuti del citato d.p.c.m. in corso di emanazione, contenente le regole tecniche per la firma, il quale si riferisce solamente alla firma digitale.

La nuova definizione di firma digitale, contenuta nell'articolo 1, comma 1, lettera n) chiarisce che si tratta di un particolare tipo di firma elettronica, con le caratteristiche proprie del sistema digitale.

Il terzo degli aspetti, che abbiamo evidenziato come cardini del regolamento, riguarda i soggetti che rilasciano la firma digitale.

Il sistema delineato dal d.p.r. n. 513/1997 era ispirato all'obiettivo di realizzare la massima sicurezza nella formazione e nell'uso del documento informatico, prevedendo una serie di cautele per l'emissione della firma digitale. Pertanto era stato stabilito un sistema di accreditamento obbligatorio, presso l'AIPA, dei certificatori, vale a dire dei soggetti abilitati a certificare le informazioni necessarie per l'utilizzo della firma digitale, ai fini del valore giuridico della stessa.

La citata direttiva europea ha obiettivi del tutto diversi da quelli delle norme italiane del 1997. Queste hanno come fine sostanziale e dichiarato l'attribuzione di specifici effetti giuridici ai documenti informatici, mentre il testo europeo è stato scritto in un'ottica di mercato<sup>7</sup>. In tal senso il legislatore

---

<sup>7</sup> Cammarata Maccarone p.5

europeo ha tracciato indirizzi diversi, perseguendo l'obiettivo della massima semplificazione e liberalizzazione dell'attività di certificazione, salva, peraltro, la previsione anche di livelli più elevati, in termini di qualità e sicurezza, delle comunicazioni telematiche<sup>8</sup>. Ne è conseguita l'esigenza per il legislatore italiano di emanare provvedimenti volti a modificare ed integrare la disciplina vigente, in modo da consentire l'uso della firma elettronica e l'emissione dei relativi certificati anche a chi non abbia richiesto autorizzazioni preventive, differenziando, peraltro, il valore delle firme e dei certificati a seconda del livello prescelto dagli interessati e del ricorso o meno alla procedura – che diviene facoltativa – dell'accreditamento dei certificatori.

Per tale motivo la normativa distingue tre diversi tipi di soggetti che rilasciano certificati di firma. La liberalizzazione di tale attività, richiesta, come detto dall'Unione europea, ha portato ad introdurre una definizione di certificatore corrispondente al “soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime” (articolo 1, comma 1, lettera u), del d.p.r.n. 445/2000).

Abbiamo, inoltre, evidenziato la necessità che la firma venga rilasciata con una tecnologia appropriata, quella cioè che la direttiva ha definito come “dispositivo sicuro di firma”<sup>9</sup>.

La normativa prevede che questa sicurezza venga garantita da un certificatore qualificato, cioè da colui il quale “rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel presente testo unico e nelle regole tecniche di cui all'articolo 8, comma 2” (art. 1, comma 1, lett. v), del d.p.r. n. 445/2000).

La medesima direttiva prevede, inoltre, sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito. Il legislatore italiano da un lato ha così previsto che “i certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati presso la Presidenza del Consiglio dei ministri-Dipartimento per l'innovazione e le tecnologie” (art. 28 d.p.r. n. 445/2000), da un altro lato ha disposto, secondo quanto già contenuto nel decreto legislativo n. 10/2002, che solo la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo sicuro, può essere utilizzata nei rapporti con le pubbliche amministrazioni (art. 38 d.p.r. n. 445/2000).

Il riconoscimento di questo livello più elevato di qualità e sicurezza, recependo la terminologia della direttiva; viene definito “accreditamento”. Con

---

<sup>8</sup> E. Granelli, *La firma digitale europea*, cit., p. 741

<sup>9</sup> la nozione di “dispositivo per la creazione di una firma sicura” è stato mutato in “dispositivo sicuro per la creazione di una firma”, riferendo l'elemento di sicurezza ad un dispositivo e non alla firma, in conformità alla “Rettifica alla direttiva 1999/93 CE del Parlamento europeo e del Consiglio del 13 settembre 1999, relativa ad un quadro comunitario per le firme elettroniche (G.U.C.E. L 13 del 19 gennaio 2000).

la medesima espressione si definisce, inoltre il procedimento (e il conseguente provvedimento conclusivo dello stesso), attraverso il quale il certificatore si accredita.

Al fine di rispettare i principi di liberalizzazione contenuti nella direttiva, ma dovendo nel contempo verificare la sussistenza dei requisiti tecnico-amministrativi necessari affinché un certificatore possa rilasciare al pubblico certificati di firma qualificati o, accreditarsi, è stata prevista l'applicazione degli articoli 19 e 20 della legge 7 agosto 1990, n. 241. In particolare per i certificatori qualificati è stata ritenuta sufficiente la dichiarazione di inizio attività (art. 19), mentre per i certificatori accreditati è stato applicato l'istituto del silenzio assenso (art. 20).

Pertanto anche la certificazione al più alto livello di qualità e sicurezza non richiede alcuna preventiva autorizzazione. Tuttavia, sull'intero settore della certificazione di firme elettroniche è stato previsto il controllo successivo sull'effettivo possesso da parte dei certificatori dei requisiti richiesti dalla normativa.

Tutto il settore del rilascio di firme digitali è stato posto sotto il controllo della Presidenza del Consiglio e più in particolare del Ministro per l'innovazione e le tecnologie, attraverso l'istituenda Agenzia nazionale per l'innovazione e le tecnologie. Il Ministro e le strutture di cui si avvale svolgono la duplice funzione di soggetti deputati a ricevere le dichiarazioni di inizio attività e di accreditamento in funzione di amministrazione attiva, nonché di soggetti deputati a svolgere attività di vigilanza sull'intero settore, in funzione di controllo (art. 29 d.p.r.).

Solo la firma, caratterizzata dai tre elementi descritti può essere definita firma con valenza giuridica analoga alla firma autografa. Ciò è quanto affermato dall'articolo 10, comma 3 del decreto legislativo n.10/2002, che riconosce alla firma digitale efficacia di prova piena fino a querela di falso<sup>10</sup>. Questa è quella che, con riferimento alla normativa comunitaria, viene definita "firma 5.1".

A questa firma non può essere invece riconosciuto il valore della firma autenticata che, secondo quanto stabilito dall'art. 20, comma 3, del d.p.r. n. 445/2000, si qualifica come tale solamente laddove vi sia l'intervento di un notaio o di un altro pubblico ufficiale a ciò autorizzato.

---

<sup>10</sup> Probabilmente in questa norma vi è stato un refuso da parte del legislatore. L'articolo 2702 riconosce alla scrittura piena prova fino a querela di falso con specifico riferimento della provenienza delle dichiarazioni da parte di chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. Attribuire al documento informatico sottoscritto con firma digitale valore fino a querela di falso in senso ampio significa riconoscere al tale firma il valore della firma autentica che, per le firme elettroniche, è invece riconosciuto dall'articolo 28 del d.p.r. n. 445/2000.

Una particolare disposizione è stata introdotta relativamente all'uso delle firme elettroniche nelle pubbliche amministrazioni. L'articolo 29-*quinquies* del d.p.r. n. 445/2000, distingue due ipotesi: l'utilizzo della firma elettronica per la sottoscrizione di documenti aventi rilevanza esterna all'amministrazione o per la sottoscrizione documenti aventi rilevanza interna all'amministrazione medesima.

Nel primo caso le amministrazioni possono acquistare, la firma digitale sul mercato, oppure possono chiedere ed ottenere il riconoscimento certificatore e rilasciare essi stessi certificati di firma digitale. Mentre la prima ipotesi costituisce la regola, la seconda possibilità rappresenta l'eccezione. Infatti le amministrazioni possono rilasciare esse stesse certificati di firma digitale a soggetti terzi, ma solo per i rapporti con l'amministrazione che ha rilasciato la firma. Ad esempio per tutto ciò che attiene la materia fiscale il Ministero dell'economia e delle finanze potrà rilasciare firme digitali ai soggetti che con essa intrattengono rapporti. Le firme che fanno uso di tali certificati però non potranno essere utilizzate ad esempio nei rapporti con un Comune anche laddove si trattasse di materia fiscale. L'elemento di distinzione è rappresentato dall'amministrazione che ha rilasciato la firma.

Per quanto riguarda i rapporti interni, le amministrazioni sono libere non solo di rilasciare ai propri dipendenti certificati di firma digitale, ma di adottare regole tecniche difformi da quelle dettate per i certificatori appartenenti al mercato.

Tali firme avranno valore, come detto solamente nell'ambito delle attività delle pubbliche amministrazioni. La norma, tuttavia, non chiarisce se tali firme possono essere utilizzate nei rapporti interni e tutte le pubbliche amministrazioni o solo nei rapporti relativi alla singola amministrazione. La norma che definisce la nozione di pubbliche amministrazioni (art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165) ha una portata talmente ampia che è ragionevole ritenere che la firma elettronica rilasciata da una pubblica amministrazione trova applicazione nei soli rapporti interni di ciascuna amministrazione. Tale interpretazione è confermata anche dal contenuto del successivo comma 3 dell'articolo 29-*quinquies*, laddove si afferma, come detto, che ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nell'emanando d.p.c.m. sulle le regole tecniche per le firme digitali.

### **Il decreto del Presidente del Consiglio recante regole tecniche per la firma digitale**

Un ultimo aspetto riguarda il decreto del Presidente del Consiglio dei ministri – del quale, come detto, si è in attesa dell'emanazione – nel quale sono

contenute le regole tecniche per la generazione, apposizione e verifica delle firme digitali, destinate a sostituire le regole tecniche precedentemente varate con decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999.

L'estrema complessità delle norme di natura tecnica necessarie per realizzare le firme digitali ha richiesto l'adozione di un ulteriore provvedimento.

In primo luogo va evidenziata l'importanza di tali regole, in quanto seppur nella liberalizzazione del settore, richiesta dall'Unione europea l'aspetto relativo alla interoperabilità delle firme assume rilievo fondamentale per assicurare l'utilizzo e la diffusione delle firme digitali.

In particolare è attraverso questo testo normativo che si delinea il confine tra firma elettronica e firma digitale. Come già detto l'utilizzo dell'espressione firme elettroniche nasce da un'precisa previsione da parte dell'Unione europea, ma, si tratta di una categoria astratta di firme. La previsione contenuta nel d.p.r 7 aprile 2003, n.137, consente di rendere sufficientemente elastica la previsione normativa in modo da non richiedere adeguamenti nell'ipotesi in cui la tecnologia introduca nuovi tipi di firme elettroniche.

Nel d.p.c.m., invece, viene compiutamente disciplinata solo la firma digitale, l'unica firma elettronica concretamente realizzabile. Il provvedimento non solo delinea la disciplina della firma digitale, ma ne detta i contenuti applicativi. Sono dettate le regole tecniche relative agli *standard* relativi alla generazione delle chiavi asimmetriche, che rappresentano la tecnologia usata per realizzare la firma digitale, le caratteristiche dei certificati di firma. La differenziazione evidenziata tra le vari categorie di certificatori ha richiesto anche l'adozione di regole tecniche di sicurezza diverse tra loro.

Per quanto riguarda il tipo di fonte normativa, l'utilizzazione di un d.p.c.m. di natura amministrativa consente un'estrema flessibilità del provvedimento, tale da consentire il tempestivo adeguamento delle regole tecniche alle mutate esigenze tecnologiche.

### **La diffusione della firma elettronica e le applicazioni imminenti**

La firma elettronica non è solo un'esercitazione di stile in quanto numerose sono le applicazioni pratiche già in atto e molte altre stanno per essere avviate.

In Italia già esistono circa 500.000 firme elettroniche, utilizzate prevalentemente da ragionieri e commercialisti nei rapporti con le Camere di commercio. A costoro la firma digitale consente di inviare alla Camera di commercio tutta la documentazione relativa alle imprese clienti.

Dopo aver definito il documento informatico ed attribuito ad esso rilevanza agli affetti di legge (art. 8 del d.p.r. n. 445/2000), la firma elettronica consente di completare gli aspetti che caratterizzano un documento.

Grazie alla firma digitale sono in corso di realizzazione numerose norme che semplificheranno i rapporti tra cittadini e imprese e pubbliche amministrazioni. per conseguire una rapida e capillare diffusione della firma digitale così da permettere ai cittadini e alle imprese di accedere con facilità e rapidità ai servizi resi dalle pubbliche amministrazioni.

Le garanzie di identificabilità del soggetto, di immodificabilità dei documenti informatici e di sicurezza, tipiche della firma digitale consentono di ampliare ulteriormente l'utilizzazione degli strumenti informatici.

L'articolo 27, comma 8, della legge 16 gennaio 2003, n. 3, recependo iniziative legislative precedentemente avviate, prevede l'adozione di regolamenti di delegificazione per la diffusione della firma digitale.

Ciò consentirà di dare attuazione alla previsione di legge in base alla quale la pubblicazione legale di bandi ed avvisi di gara non avverrà più sulla gazzetta ufficiale ma su siti informatici (art. 24, legge 24 novembre 2000, n. 340); sarà possibile utilizzare la posta elettronica disponibile sui normali personale computer con un valore giuridico analogo alla posta raccomandata (art. 14, d.p.r. n. 445/2000).

I relativi provvedimenti attuativi - quello per la pubblicazione legale di bandi ed avvisi di gara su siti informatici, approvato dal Consiglio dei ministri il 16 maggio 2003, e quello concernente la posta elettronica certificata 2003, in corso di approvazione -saranno pubblicati in tempi brevi.

(pubblicato in [www.astridonline.it](http://www.astridonline.it) il 16 giugno 2003)