www.contabilita-pubblica.it

SAPIENZA
UNIVERSITÀ DI ROMA

Facoltà di Giurisprudenza
Dipartimento di Scienze giuridiche

Master universitario di II livello in
"Diritto dell'Informatica e Teoria e Tecnica della Normazione"

L'EVOLUZIONE TECNICA DELLA FIRMA DIGITALE: GLI EFFETTI SULL'ORDINAMENTO GIURIDICO ITALIANO

Relatore

Chiar.mo Prof. Donato Limone

Candidato

D.ssa Antonella Zammitti

Anno accademico 2008/2009

01/12/2010

Introduzione

Il presente lavoro si propone di analizzare in modo dettagliato uno degli strumenti più rilevanti del processo di informatizzazione iniziato diversi anni fa con l'ingresso delle nuove tecnologie dell'informazione e della comunicazione (*Information and Communication Technology*[1]), ma che vede le sue applicazioni pratiche e tangibili soprattutto di recente.

La diffusione delle tecnologie informatiche e telematiche, infatti, ha posto con pressante urgenza la necessità di sostituire il tradizionale documento cartaceo con un equivalente strumento informatico, che fosse in grado di assicurare la stessa validità probatoria e di garantirne l'autenticità e la paternità. E' da questa esigenza che nasce il concetto di firma digitale, intesa come unico ed affidabile strumento capace di sostituire la sottoscrizione autografa, che sino ad ora aveva rappresentato l'elemento base per garantire la certezza di un qualsiasi atto, ed offrire in tal modo maggiori garanzie sulla sicurezza dei documenti informatici, facilitando la diffusione dei negozi giuridici telematici.

L'introduzione di questo nuovo istituto ha creato, però, molti problemi, primo fra tutti quello del suo inquadramento giuridico. Ciò ha costretto dapprima il giurista a ricercare analogie e differenze rispetto agli istituti tradizionali, e successivamente il legislatore a modificare radicalmente la configurazione giuridica degli istituti esistenti per adattarla alle nuove realtà.

Come si vedrà, l'approccio culturale al fenomeno, pur prevedendo l'introduzione di una normativa specifica di settore, necessaria per dare valore legale alle innovazioni, ha inteso riallacciarsi alle categorie tradizionali del diritto. Nel corso di questo studio si evidenzierà come le scelte seguite al riguardo dal legislatore italiano hanno suscitato numerose obiezioni dottrinali e giurisprudenziali.

Non va dimenticato poi che la firma digitale, assieme ad altre innovazioni quali il documento informatico, il procedimento amministrativo elettronico e la posta elettronica certificata, hanno svolto un ruolo decisivo nel processo di trasformazione della pubblica amministrazione in amministrazione "digitale", andando a toccare più fronti: normativo, organizzativo e soprattutto tecnologico.

Non si è trattato solo di perseguire esigenze di celerità, trasparenza ed efficienza dell'attività amministrativa, nel solco già indicato da tempo a partire dalla L. n. 241/90, ma anche di fornire garanzie più elevate in relazione alla certezza dei documenti amministrativi nella forma elettronica, ormai dotati di un livello di sicurezza tale da rendere estremamente difficili contraffazioni o usi indebiti e quindi tutelare quanti abbiano fatto affidamento su di essi.

Sebbene nella maggior parte delle P.A. tali strumenti si limitino attualmente ad affiancare i tradizionali modelli di gestione dei procedimenti amministrativi, essi sono destinati a diventare in futuro il solo *modus operandi*. A tal fine sarà necessario, tuttavia, mutare gli indirizzi e le procedure

[1] Da adesso: I.C.T.

operative della P.A., cercando di superare le barriere giuridico- istituzionali che si frappongono, per dare priorità ad esigenze di carattere funzionale-organizzativo.

Una delle ragioni che non permettono di procrastinare ulteriormente tale processo di cambiamento, e che interessa in modo particolare le strutture pubbliche, risiede nell'esigenza di dematerializzazione della documentazione, vale a dire il progressivo e definitivo passaggio dalla carta al digitale, destinato ad incidere profondamente sul cd. *back office*.

Nei processi di dematerializzazione dei documenti e di fatturazione elettronica la firma digitale è l'elemento fondamentale che fornisce al documento informatico la stessa validità legale del documento cartaceo sottoscritto. A riguardo la Deliberazione C.N.I.P.A.[2] n. 11/2004 è dedicata alla conservazione digitale della documentazione della Pubblica Amministrazione e dei privati, processo finalizzato a rendere un documento facilmente reperibile, non deteriorabile e quindi accessibile e disponibile nel tempo in tutta la sua integrità e autenticità[3].

L'elaborato si compone di due capitoli, il primo dei quali delinea le tappe principali che hanno caratterizzato l'affermazione della firma digitale e fornisce una ricostruzione per grandi linee dell'evoluzione storica della materia.

Nel secondo capitolo, invece, vengono esaminati i concetti fondamentali e le tecnologie su cui la firma digitale si basa, viene descritto il processo che conduce alla creazione della stessa e viene compiuta una analisi delle recentissime modifiche intervenute in tema di validità temporale, anche in prospettiva delle applicazioni future.

La presente dissertazione si chiude con le conclusioni finali che riportano alcune delle problematiche che a tutt'oggi risultano essere un ostacolo all'affermazione della firma digitale e le misure che potranno essere predisposte per accelerarne la diffusione.

[2] Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

[3] Ciò si rende possibile per mezzo degli strumenti della firma digitale e del riferimento temporale, che consentono di eseguire la conservazione dei documenti anche su supporti persistenti (es. *hard-disk*, *floppy-disk*, nastri ecc.), garantendo la sicurezza della procedura di conservazione e la verifica di integrità. Inoltre, l'ingresso di queste nuove figure giuridiche permetterà la lavorazione delle pratiche e la loro archiviazione sui suddetti supporti aventi il pregio di essere di dimensioni ridotte e di poter contare su una flessibilità gestionale elevatissima.

1. L'evoluzione normativa della firma digitale: brevi cenni

1.1 La disciplina italiana

La regolamentazione normativa della firma digitale trova le sue prime basi nel D. Lgs. n. 39/93, che disciplina la progettazione, lo sviluppo e la gestione dei sistemi informativi automatizzati delle amministrazioni dello Stato, seppur limitandosi ad enunciare norme di principio o di programma[4].

Visto l'ambito della trattazione di questo lavoro, tralasceremo di soffermarci sulle molteplici norme che sono intervenute in materia, in modo del tutto frammentario, per esaminare nel dettaglio quelle che hanno segnato i passaggi fondamentali per lo sviluppo della firma digitale.

Nel 1997 si assiste all'introduzione della disposizione normativa intorno alla quale ruota l'intero settore del diritto dell'informatica. Si tratta dell'art. 15, 2° co. della legge 15 marzo 1997 n. 59 (cd. Legge Bassanini), che così statuisce: "*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 strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*". Viene in tal modo sancito, per la prima volta nel nostro ordinamento, "*il principio di generale rilevanza e validità dell'attività giuridica in forma elettronica: gli atti pubblici e i negozi privati emanati e stipulati mediante l'utilizzo di sistemi informatici e telematici, sono dunque validi e rilevanti a prescindere dalla loro trasposizione su supporto cartaceo, che ove presente, costituisce copia del documento (originale) informatico*"[5]. Ciò significa che il supporto su cui è registrato il documento diventa irrilevante, mentre acquista valore il contenuto[6].

Tale norma statuisce altresì la necessaria conformità delle procedure informatiche e telematiche ad apposite regole tecniche[7] fissate dall'A.I.P.A., ora divenuta C.N.I.P.A.[8].

---

[4] Ne è un esempio l'art. 3 del citato decreto da cui si evince l'ammissibilità, a livello di principio generale, della manifestazione all'esterno, rappresentazione e perfezionamento dell'atto amministrativo elettronico, per mezzo di modalità elettroniche di formalizzazione del contenuto. Tale articolo è stato oggetto di numerose critiche da larga parte della dottrina, a causa di alcune rilevanti omissioni in materia di firma e della conseguente inidoneità a fornire adeguate garanzie di autenticità e quindi di validità degli atti, ai fini dell'imputabilità giuridica del documento informatico. Vedi al riguardo Minerva M., *L'attività amministrativa in forma elettronica* , in *Foro. Amm.*, 1997, 04, 1304; Duni, *Le firme elettroniche nel diritto vigente*, in *Dir. Informazione e Informatica*, 2006, 4-5, p. 506; Borruso R., *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (D. Lgs. 23 gennaio 2002 n. 10, D.P.R. 7 aprile 2003 n. 137 e L. 29 luglio 2003 n. 229*, in *Giust. Civ.*, 2004, n. 3, p. 145.

[5] Minerva M., *L'attività amministrativa in forma elettronica* , in *Foro. Amm.*, 1997, 04, 1307.

[6] Dal punto di vista tecnico quanto detto è il risultato della normale scorporabilità dei *bit*, registrati su qualsiasi supporto leggibile con strumenti informatici, dal supporto medesimo e la possibilità di trasferirli su altri supporti .

[7] Ciò era stato disposto, con riguardo alle pubbliche amministrazioni, dall'art. 7 co. 1 lett. a del già richiamato D. Lgs. n. 39/93.

Tale conformità viene richiesta allo scopo di garantire l'interoperabilità tra i sistemi e le applicazioni, pubbliche e private, che permettano di realizzare transazioni giuridicamente rilevanti in forma elettronica. Le pubbliche amministrazioni ed i privati, infatti, devono poter far riferimento quanto meno a procedure uniformi, in particolare con riguardo alla firma elettronica, che consentano loro l'adozione di un sistema unico di sottoscrizione elettronica[9]. Parimenti è importante che vi sia uniformità dei criteri di generazione, conservazione e certificazione delle chiavi, mentre è ammessa una certa flessibilità con riguardo alle realizzazioni, ai prodotti e alla lunghezza delle chiavi, variabili a seconda delle diverse esigenze.

La disciplina in materia subisce un impulso fortemente innovativo con il D.P.R. n. 513/97[10], al quale va riconosciuto il merito di aver sancito l'equiparabilità della firma digitale alla sottoscrizione autografa in linea generale e non solo limitatamente a casi specifici come era accaduto in passato. Ciò avviene, in particolare, grazie alla previsione del sistema crittografico a chiavi asimmetriche, di cui si parlerà meglio nel prosieguo. Basti dire per ora che, attraverso l'impiego di tali tecnologie, è stato possibile riconoscere piena efficacia probatoria al documento informatico, sia dal punto di vista della provenienza, e quindi dell'imputabilità, sia da quello dell'integrità del contenuto.

Vanno citati a tale proposito alcuni articoli del regolamento contenenti importanti novità, molte delle quali sono sopravvissute nel Codice dell'Amministrazione Digitale, attualmente in vigore e sistema normativo di riferimento in materia[11].

Una di queste è la definizione di documento informatico quale "… *rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"* [12].

Il decreto in esame attribuisce al *"...documento informatico, sottoscritto con firma digitale, efficacia di scrittura privata ai sensi dell'art. 2702 c.c."*, in tal modo viene conferita l'efficacia formale della scrittura privata ad un documento diverso sotto l'aspetto ontologico[13]. Si precisa, poi

---

[8] Con il D. Lgs. 39/93, istitutivo dell'Autorità per l'Informatica nella Pubblica Amministrazione, a dispetto della denominazione *"Autorità"*, essa veniva posta alle dipendenze del Governo. In seguito, con la L. 675/96 si è affermato che "*l'Autorità opera in piena autonomia e con indipendenza di giudizio e di valutazione"*. Da ultimo il D. Lgs. n. 196/2003 ha disposto la sostituzione del termine A.I.P.A. con quello di C.N.I.P.A. e ha precisato che il "*Centro Nazionale per l'Informatica nella P.A. opera presso la Presidenza del Consiglio dei Ministri*". Ne ha specificato altresì il fine: "*l'attuazione delle politiche del ministero per l'Innovazione*", sacrificandone così, almeno sulla carta, l'indipendenza. Nel momento in cui si scrive il D. Lgs n. 177/09 ha attuato una riorganizzazione del C.N.I.P.A., trasformandolo in DigitPA, l'ente pubblico non economico che ne assume le funzioni.

[9] Individuato di lì a poco nella crittografia a chiave asimmetrica.

[10] Recante "criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici".

[11] Contenuto nel D. Lgs. n. 82/2005 ed entrato in vigore il 1 gennaio 2006. Da adesso: C.A.D. o Codice.

[12] Sostituendo così il termine "supporto", previsto nell'art. 491-bis c.p. introdotto dalla L. 547/93, con quello più corretto di "rappresentazione", tendente a configurare una nuova forma di "scrittura" caratterizzata dalla registrazione in *bit*, ma comparabile quanto a valore a quella tradizionale. Con tale precisazione terminologica, il legislatore del 1997 ha voluto evidenziare, in realtà, che la sottoscrizione su un documento informatico, formata dall'indicazione del proprio nome e cognome, ancorché autografa, non è affidabile, data la possibilità di prelevare tale firma dal documento e travasarla in calce ad un altro. Ne deriva che per assicurare l'imputabilità dello scritto è necessario avvalersi dei nuovi tipi di firma, in grado di offrire garanzie equivalenti a quelle della firma autografa.

[13] La scrittura privata è infatti la dichiarazione scritta che reca la firma autografa del dichiarante, mentre la firma digitale viene definita dal regolamento stesso come il risultato della procedura informatica basata sul sistema di chiavi asimmetriche a coppia, una pubblica e una privata.

che "*l'apposizione o l'associazione della firma digitale al documento informatico, equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo*"[14].

La firma digitale perciò assurge a strumento di imputazione al sottoscrittore della dichiarazione contenuta nel documento. Essa, pur avendo gli stessi effetti della sottoscrizione tradizionale, si contraddistingue per la sua idoneità ad essere apposta a un documento informatico o ad un gruppo di documenti informatici, nonché al duplicato o copia di atti o essere associata al documento informatico con separata evidenza informatica, come previsto dal co. 1° del citato art.10. In ultimo, i commi 5° e 7° forniscono ulteriori certezze in merito alla paternità della firma digitale[15].

Allo stesso modo, in relazione ai documenti informatici della pubblica amministrazione, si dispone che "*..la firma autografa o la sottoscrizione comunque prevista è sostituita dalla "firma digitale"*[16]. Ciò significa che le due tipologie di firma hanno valore equivalente e che la firma digitale sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi previsti dalle discipline di settore.

Dunque, anche nella P.A. la piena validità e rilevanza del documento informatico viene subordinata al rispetto di determinate regole tecniche riguardanti la sua formazione, che sono in parte dettate dallo stesso regolamento. Per la restante disciplina il decreto in esame prevedeva, entro centottanta giorni dalla sua entrata in vigore, l'emanazione in capo al Governo, con D.P.C.M., di un regolamento contenente le regole tecniche per la formazione, trasmissione e archiviazione, di documenti con strumenti informatici e telematici, ma queste videro la luce solo nel 1999[17].

Il successivo passaggio normativo si ebbe nell'anno 2000 quando il D.P.R. n. 513/97 venne abrogato e integralmente trasfuso nel D.P.R. n. 445/00, vale a dire il "Testo Unico in materia di Documentazione Amministrativa"[18], mantenendo in vigore le regole tecniche pocanzi menzionate. A fondamento delle norme suddette permane, secondo la dottrina, la stessa *ratio*, vale a dire il pieno riconoscimento giuridico della documentazione informatica e la sua equiparazione alla tradizionale documentazione cartacea[19].

Tale quadro normativo era destinato ad essere messo in discussione dalla direttiva 1999/93/Ce, alla quale il legislatore italiano fu chiamato a dover dare attuazione.

[14] Artt. 5 e 10 del D.P.R. n. 513/97.

[15] La firma digitale deve infatti riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme dei documenti cui è apposta o associata; attraverso di essa devono potersi rilevare gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

[16] Art.19 del D.P.R. n. 513/97.

[17] Con il D.P.C.M. 8 febbraio 1999.

[18] Da adesso: T.U.D.A. o D.P.R. 445/00.

[19] Contaldo A., *Il documento informatico e la firma digitale nella pubblica amministrazione: appunti per una ricostruzione della fattispecie*, in *Riv. Amm. della Rep. It.*, 1-2, 2002, p. 45.

1.2 La disciplina comunitaria e i problemi legati al recepimento interno

L'adeguamento alla sopravvenuta direttiva comunitaria del Parlamento e del Consiglio Europeo sulle firme elettroniche, che portò alla modifica del citato D.P.R. n. 445/00, avvenne per opera del D. Lgs. n. 10 del 2002[20], a cui seguì poco dopo il D.P.R. n. 137/03[21].

Per comprendere le modifiche introdotte dalla direttiva comunitaria è necessario spiegare le scelte politiche che ne stanno alla base. L'intento della Comunità europea è stato in primo luogo quello di liberalizzare il mercato dei certificatori, attribuendo comunque ad ogni Stato membro il potere di regolamentare ed accordare il rilascio di quelle firme generate attraverso l'uso di dispositivi sicuri ed alle quali viene quindi riconosciuta efficacia probatoria privilegiata[22].

In secondo luogo, come affermato nell'art. 4, essa ha voluto favorire la libera circolazione nello spazio giuridico comunitario delle firme elettroniche conformi alla direttiva.

La liberalizzazione del mercato dei certificatori, seppur non investe quelle firme dotate di efficacia probatoria particolarmente elevata, porta alla conseguenza che chiunque, senza alcun preventivo controllo o autorizzazione pubblica, può prestare al pubblico servizi di certificazione e quindi autenticare le firme che lui stesso mette in circolazione[23].

È stato giustamente rilevato in dottrina[24] che, seppur lo scopo del legislatore comunitario sia quello di privilegiare il profilo economico-imprenditoriale, consentendo a tutti gli operatori di trarre profitto da questa attività, ciò va a discapito della sicurezza dei traffici commerciali e della circolazione dei beni. Infatti, "*l'intero sistema della firma digitale fa perno sull'affidabilità tecnica e morale del certificatore*[25]*, vi è quindi un poderoso interesse pubblico a che chi esercita questa attività, pur in regime di libera concorrenza, lo faccia dopo aver dimostrato di possedere imprescindibili requisiti che ne giustifichino l'affidamento*"[26].

[20] Con la "Legge comunitaria 2000" n. 422 il Parlamento ha delegato il Governo a recepire la direttiva europea, il che è avvenuto con il menzionato D. Lgs. n. 10/02.

[21] "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'art. 13 del decreto legislativo 23 gennaio 2002, n. 10".

[22] Al riguardo l'art. 3 dispone che "Gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione" e che "..possono introdurre o conservare sistemi di accreditamento facoltativi volti a fornire servizi di certificazione a livello più elevato"

[23] A differenza di quanto prescritto dal D.P.R. 513/97 che, prevedendo unicamente la firma digitale, autorizzava il rilascio dei dispositivi e dei certificati per generarla solo ai soggetti forniti di particolari requisiti ed accreditati con iscrizione in uno specifico albo presso l'A.I.P.A. (i certificati così originati, essendo dotati di un elevato livello di sicurezza, vennero definiti "qualificati").

[24] Graziosi A., *La nuova efficacia probatoria del documento informatico*, in *Rivista trim. di dir. proc. civ.* , 2003, 01, p. 55.

[25] Definito dagli informatici t.p.f. che sta per "terza persona fidata" dall'espressione inglese "*trusted third part*", generalmente nota come Autorità di Certificazione, dall'espressione inglese *Certification Authority*.

[26] Graziosi A., Ibidem, in *Rivista trim. di dir. proc. civ.* , 2003, 01, p. 55.

1.2.1 Firma digitale e firme elettroniche

L'opera di adeguamento dell'ordinamento italiano a quello comunitario è stata realizzata dal D. Lgs. n. 10/02 attraverso la sostituzione del contenuto di alcuni articoli del D.P.R. n. 445/00 e l'introduzione di altri *ex novo,* tecnica che ha fatto sorgere numerose contraddizioni, stante la differente impostazione tra le due legislazioni e la confusione generata dalla nuova nomenclatura introdotta dalla normativa europea[27].

In questa sede, per ragioni di spazio, si è limitata l'analisi ad alcuni articoli oggetto di novellazione. Va esaminato preliminarmente l'art. 2 del D. Lgs. citato, mentre gli altri saranno presi in considerazione più avanti. Il testo dell'art. 2 definisce la "firma elettronica" come "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici*[28]*, utilizzati come metodo di autenticazione informatica*" e prosegue specificando che si intende per "firma elettronica avanzata" 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"*[29].

È stato osservato da più parti[30] che, mentre il legislatore comunitario decise di avvalersi di un sistema tecnologicamente neutro, basato sulla libertà di scelta di qualunque mezzo elettronico[31] di identificazione, a cui riconoscere validità giuridica[32], il legislatore italiano preferì sin dal D.P.R. n. 513/97 ammettere come unico sistema di firma elettronica quello a chiavi asimmetriche[33], non solo

[27] Firma elettronica anziché firma digitale.

[28] Va precisato che per firma "allegata ai dati" si intende la firma contenuta nello stesso *file*, ad esempio in calce al documento; mentre per firma "ad essi connessa tramite associazione logica" ci si riferisce alla firma contenuta in un *file* diverso. Entrambi i casi rappresentano comunque metodi di associazione fra firma elettronica e documento.

[29] La particolarità della firma elettronica rispetto a quella tradizionale sta proprio nel fatto di non essere qualcosa di fisso ed immutabile. La firma elettronica nasce nel momento in cui esiste un documento da firmare; ne consegue l'impossibilità di firmare un foglio in bianco.

[30] Contaldo A., *Il documento informatico e la firma digitale nella pubblica amministrazione: appunti per una ricostruzione della fattispecie*, in *Riv. Amm. della Rep. It.*, 1-2, 2002, p. 49; Duni G., *Le firme elettroniche nel diritto vigente*, in *Dir. Informazione e Informatica*, 2006, 4-5, p. 507; Santangelo E., Nastri M., *Firme elettroniche e sigilli informatici*, in *Vita Notarile*, 2002, 2, p. 1122.

[31] Infatti, il significato del termine "elettronico" è stato usato perché più ampio di "informatico", in quanto i segnali elettronici possono essere tanto "digitali" (o "numerici" perché costituiti dai numeri 0 o 1, cioè da *bit*, quanto "analogici" (cioè misurabili solo per analogia con altri fenomeni non elettronici). Questa è la ragione per cui la direttiva europea ha usato la nuova nomenclatura di firma elettronica, anziché digitale. Il legislatore comunitario ha voluto in tal modo lasciare spazio all'evoluzione tecnologica e consentire l'eventuale ingresso di nuovi strumenti tecnologici.

[32] Le proprietà della firma elettronica avanzata, infatti, potrebbero essere garantite anche dall'adozione di tecnologie diverse dalla crittografia a chiavi asimmetriche.

[33] Questo sistema si avvale di due chiavi complementari: una usata per cifrare, definita privata, l'altra per decifrare, definita pubblica. La chiave privata è usata per cifrare l'impronta di un documento, la corrispondente pubblica per decifrare l'impronta e confrontarla con quella del documento. Tale sistema permette di garantire la provenienza (la chiavi pubblica è legata ai dati anagrafici di una persona fisica) e l'inalterabilità del documento attraverso l'uso combinato delle due chiavi. Tale sistema crittografico fu creato da due matematici, Diffie e Helmann, e perfezionato, sotto il profilo della funzione di "firma" (nel senso di attribuibilità del documento a colui

per le garanzie di sicurezza fornite dal punto di vista tecnologico, ma anche per quelle derivanti dalle tecniche di gestione ed erogazione degli strumenti.

La normativa comunitaria configura, dunque, secondo la dottrina maggioritaria, due diverse tipologie di firme elettroniche. Ritroviamo nella lettera a del citato art. 2 del D. Lgs. n. 10/02 quella che viene comunemente definita "semplice" o "leggera", essendo priva di garanzie quanto all'identificazione del titolare, alla connessione univoca allo stesso e quindi dotata di una minore rilevanza sostanziale e probatoria; e alla lettera g quella "avanzata", in quanto provvista di tutti questi elementi e caratterizzata da alti standard tecnici di sicurezza in grado di assicurare una maggiore valenza giuridica[34].

Da più parti si ritiene[35] che la firma avanzata prevista dalla direttiva corrisponda sostanzialmente alla firma digitale basata sul sistema delle chiavi asimmetriche già disciplinata dal legislatore italiano nel 1997; mentre la firma cosiddetta "semplice", cioè la firma non generata con un dispositivo sicuro e mancante di un certificato qualificato, corrisponda ad un qualunque sistema di identificazione telematica, che pur fornendo un basso livello di sicurezza, non va disconosciuto dagli Stati appartenenti alla CE [36].

Ne deriva una diversa efficacia giuridica delle due firme: "*la firma digitale è equivalente a una sottoscrizione autografa. Le altre potrebbero non esserlo: vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza …*"[37].

---

che lo aveva criptato), da Rivest , Shamir e Adelman, da cui prese il nome acronimo di sistema RSA, usato ancora oggi per indicare la firma digitale realizzata a mezzo della criptazione asimmetrica.

[34] Si può notare che in realtà la funzione di identificazione dell'autore della firma e la connessione univoca allo stesso non consentono di identificare chi appone materialmente la firma, cioè chi fa uso del dispositivo per la creazione della firma, ma si limitano ad individuare il soggetto che ne risulta titolare. Cfr. sull'argomento Finocchiaro G., *La direttiva relativa a un quadro comunitario per le firme elettroniche,* in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 639.

[35] Si pensi tra i tanti a Bianca C. M., *La firma elettronica: si apre un nuovo capitolo,* in *Studium Iuris*, 2002, p. 1432; Santangelo E., Nastri M., *Firme elettroniche e sigilli informatici*, in *Vita Notarile,* 2002, 2, p. 1122; Lisi A., *Dal CNIPA un po' di chiarezza su firme elettroniche "leggere" e "pesanti": User Id" e "Pw" possono essere firma elettronica leggera!,* in *http: //www.jei.it/infogiuridica/notizia.php?ID_articoli=343*, 9-06-2004. Quest'ultimo precisa che qualora non si configuri una firma digitale "*…più che di un processo di firma si tratta di un processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria*".

[36] Ad esempio nel commercio elettronico si utilizzano semplicemente *username* e *password* che, come i *pin* si basano un sistema a chiavi simmetriche, in cui la chiave di criptazione (che serve anche per decriptare) è quasi sempre conosciuta da più di un soggetto o, in ogni caso, è il più delle volte, facilmente ricavabile tramite appositi *software*. Anche il C.N.I.P.A. conferma questa impostazione dottrinale, in linea con lo sviluppo del commercio elettronico, precisando che "*la firma elettronica (generica) può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici*" (*Linee Guida per l'utilizzo della Firma Digitale*, in *http://www.cnipa.gov.it/site/_files/LineeGuidaFD_200405181.pdf*, Maggio 2004).

[37] Questa tesi sposata dal C.N.I.P.A. giunge a considerare idonei strumenti di autenticazione in grado di attribuire forma scritta ai documenti informatici di riferimento, anche se liberamente valutabili dal giudice dal punto di vista probatorio:

- gli accessi in un'area riservata di un sito *web* al fine di autenticare tutte le future transazioni da effettuare *on line*
- le *e-mail*
- la spedizione telematica delle dichiarazioni dei redditi (Entratel del Ministero dell'Economia)
- l'operazione di attestazione nel progetto CRS-SISS della Regione Lombardia

Secondo un'autorevole dottrina la firma digitale, più precisamente, non viene sostituita dalla firma elettronica avanzata, ma viene in essa inglobata, in quanto "*realizzata con una chiave (quale, appunto, quella "privata") sulla quale il firmatario – cioè l'autore del messaggio – conserva un controllo esclusivo e collegata ai dati ai quali si riferisce (cioè al testo del documento informatico) in modo da impedirne qualsiasi alterazione*"[38].

Tale impostazione si ritrova, seppur diversamente articolata, in un altro orientamento dottrinale[39], che ravvisa nell'art. 10, co. 3°, del D.P.R. n. 445/00, così come modificato dal D. Lgs. n.10/02, due differenti fattispecie: il documento informatico sottoscritto con firma digitale e il documento informatico sottoscritto con firma elettronica avanzata, basata su un certificato qualificato[40] e generata mediante un dispositivo per la creazione di una firma sicura[41].

L'autore evidenzia come la prima delle due fattispecie, già regolata dal D.P.R. n. 445/00 (e in precedenza dall'art. 5 D.P.R. n. 513/97) che le riconoscevano efficacia di scrittura privata ex art. 2702, trae vantaggio dalla nuova disciplina, che attribuisce al documento informatico sottoscritto con firma digitale l'efficacia di piena prova fino a querela di falso, mettendolo a riparo dalla possibilità di un suo disconoscimento[42].

Con riguardo alla seconda fattispecie, quasi interamente ripresa dagli artt. 2 e 5 della Dir. 1999/93, osserva l'autore come essa configuri "*una sorta di protocollo di sicurezza delle firme elettroniche – costituito dalle tre unità fondamentali, della firma elettronica avanzata, del certificato qualificato e del dispositivo di firma sicura*" – e conferisca efficacia di piena prova fino a querela di falso "*a qualunque firma si dimostri rispettosa di questo standard di sicurezza*"[43].

Si può osservare come il legislatore abbia in tal modo adottato, anche con riferimento alle firme elettroniche a cui viene riconosciuta la massima efficacia probatoria, un sistema tecnologico neutro che, in conformità con i principi comunitari, consente di accogliere qualsiasi prodotto informatico in

– alcune sottoscrizioni che avvengono senza *smart card* nei processi di *e-banking* ecc.. Lisi A., *Dal CNIPA un po' di chiarezza su firme elettroniche "leggere" e "pesanti": User Id" e "Pw" possono essere firma elettronica leggera!*, in *http: //www.jei.it/infogiuridica/notizia.php?ID_articoli=343*, 9-06-2004. Ai sensi del nuovo co. 1° bis art. 20 del C.A.D. l'idoneità del documento informatico a soddisfare il requisito della forma scritta è soggetta alla valutazione del giudice, la quale tiene conto, oltre alle caratteristiche oggettive di qualità e sicurezza, anche di quelle inerenti l'integrità e l'immodificabilità, cfr. sul punto 2.3.5.1.

[38] Borruso R., *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (D. Lgs. 23 gennaio 2002 n. 10, D.P.R. 7 aprile 2003 n. 137 e L. 29 luglio 2003 n. 229)*, in *Giust. Civ.*, 2004, n. 3, p. 151 e ss.

[39] Graziosi A., *La nuova efficacia probatoria del documento informatico*, in *Rivista trim. di dir. proc. Civ.*, 2003, 01, p. 57.

[40] Definiti dallo stesso art. 2 come 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.

[41] Vale a dire l'apparato strumentale usato per la creazione di una firma elettronica, rispondente ai requisiti di cui all'articolo 10 del citato D. Lgs. n. 10/02, così come stabiliti dall'allegato III della direttiva 1999/93/CE.

[42] Tale efficacia probatoria ha subito ad oggi alcune modifiche, secondo quanto previsto dal nuovo art. 21 co. 2° del C.A.D.. Si veda al riguardo il par. 2.3.5.1, 2° capitolo.

[43] Graziosi A., Ibidem, in *Rivista trim. di dir. proc. civ.* , 2003, 01, p. 57.

linea con le specifiche tecniche previste dagli allegati I e II della direttiva e con le regole tecniche fissate con D.P.C.M., previa valutazione da parte di un organo creato ad hoc[44].

Tuttavia la dottrina più attenta ha evidenziato altresì come l'errata traduzione della direttiva calata nell'ordinamento italiano ha generato numerose incomprensioni, che non consentono di ricondurre *sic et simpliciter* le diverse tipologie di firme esistenti a quelle ora esaminate[45].

Si è osservato, a questo proposito, come la *firma elettronica avanzata* contemplata dall'art. 2 del D. Lgs. n. 10/02, pur prevedendo la validazione dell'identità del firmatario, non corrisponde alla definizione di firma digitale in senso stretto quale introdotta dal D.P.R. n. 513/97, essendo priva di riferimenti al certificato qualificato e al dispositivo sicuro. Questo tipo di firma, infatti, non necessita di un certificato qualificato per collegarla unicamente al firmatario, essendo altamente improbabile che la stessa coppia di chiavi sia attribuita a due soggetti diversi; ne discende l'idoneità a confermare l'identità del firmatario. In secondo luogo, la sua creazione con mezzi sui quali il firmatario può conservare un controllo esclusivo si attua semplicemente mantenendo segreta la chiave privata e il PIN che attiva la procedura. In ultimo, è collegata ai dati in modo che sia possibile rilevare un qualsiasi cambiamento degli stessi successivo alla generazione della firma[46]. Ne consegue che, secondo l'impostazione ora esaminata, tale firma avrebbe dovuto essere più chiaramente identificata come "leggera" o "debole" che dir si voglia.

In quest'ottica, quindi, essendo le firme caratterizzate dalla doppia funzione di validazione dei dati e del firmatario, vengono escluse dal novero le cosiddette segnature elettroniche, che si limitano alla semplice validazione dei dati[47]. Eppure il legislatore italiano ha omesso di definire la semplice validazione dei dati e ha erroneamente configurato la *electronic signature*, prevista dalla direttiva comunitaria, come una firma elettronica "debole"[48] e la *advanced electronic signature* come una firma digitale "forte", dimenticando che anche quest'ultima può degradare ad una firma "debole" in mancanza dei requisiti di sicurezza sopra indicati, pur se dotata del requisito del controllo esclusivo[49]. Questo errore di traduzione discende dal fatto che la firma digitale "forte" non trova una definizione specifica nella normativa europea . Nonostante l'art. 5 della direttiva 1999/93 precisi che le *firme elettroniche avanzate* basate su un certificato qualificato e generate con un dispositivo sicuro soddisfano i requisiti legali di una firma in relazione ai dati in forma elettronica così come la firma autografa soddisfa quei requisiti in relazione a dati su carta e che siano ammesse come prova in

[44] Si tratta del Dipartimento per l'innovazione e le tecnologie (DIT) istituito presso la Presidenza del Consiglio dei Ministri, ex artt. 3, 4, 5 del D. Lgs. n. 10/02.

[45] Cammarata M., *Firme elettroniche, problemi normativi del documento informatico*, Monti & Ambrosini ed., 2007, p 42 e ss.

[46] Va ricordato, al riguardo, che la firma elettronica, avanzata o meno, fornisce comunque la certezza dell'integrità del documento, permettendo di sapere se lo stesso abbia subito alterazioni.

[47] Si pensi ad esempio alla filigrana, ai codici di controllo come il codice a barre ecc.

[48] Cioè non certificata da un certificatore accreditato e quindi non equivalente a una firma autografa, con conseguente impossibilità di applicare il disposto dell'art. 2702 c.c.. Ciò si ricava anche dagli artt. 21, co. 1° e 23 del C.A.D., i quali stabiliscono rispettivamente che il documento con firma elettronica è liberamente valutabile dal giudice e quello privo di firma è inserito tra le riproduzioni meccaniche.

[49] Cammarata M., Ibidem, Monti & Ambrosini ed., 2007, p 42 e ss.

giudizio[50], queste firme sono considerate dal legislatore comunitario semplicemente come una specie della segnatura avanzata (di cui all'art. 2 della Dir.). Il che deriva probabilmente dalla scelta di un approccio tecnico e informatico, in base al quale firma "debole" e firma "forte" sono equivalenti, nel senso che danno la stessa certezza "matematica" dell'integrità del testo[51]; ciò che le differenzia è la presenza di elementi esterni all'ambito tecnologico che servono per conferire "certezza legale" circa l'attribuzione della firma digitale a un determinato soggetto[52] e quindi consentire l'equiparazione degli effetti della firma digitale "forte" a quelli della firma autografa[53].

Ne consegue che il legislatore italiano, nell'intento di ottenere una firma digitale "forte", equivalente a quella già prevista dall'ordinamento interno, ha sommato i requisiti previsti dalla direttiva all'art. 5 (certificato qualificato e dispositivo sicuro) alla definizione di *advanced electronic signature* (firma debole) di cui all'art. 2, ottenendo in tal modo la *firma elettronica qualificata*, aggettivo non presente nella direttiva.

Il risultato si ritrova dapprima nel D.P.R. n.137/03[54] e poi nell'attuale art. 1 lett. r del C.A.D., così come modificato dal D. Lgs. n. 159/2006, che definisce la *firma elettronica qualificata* quale:

"*la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario [e la sua univoca autenticazione informatica] , 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, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma [quale l'apparato strumentale usato per la creazione della firma elettronica]*"[55].

Anche la *firma elettronica*, a seguito del D. Lgs. correttivo del 2006, trova nel C.A.D. all' art. 1 lett. q una nuova definizione: "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*". La

[50] Equiparando così firma autografa e firma digitale "forte".

[51] La crittografia asimmetrica, infatti, si avvale dell'impronta del documento, realizzata attraverso la funzione di *hash*, che consente di verificare l'integrità dello stesso. Tale tecnologia contraddistingue anche una firma elettronica "debole", se per debole si intende "priva del certificato qualificato o del dispositivo sicuro". Esulano dal campo le firme elettroniche che non garantiscono neanche l'integrità, così i sistemi basati sulla crittografia simmetrica (es. *user-id* e *password*).

[52] L'autore si riferisce ancora una volta alla presenza della certificazione dell'attribuzione della coppia di chiavi a un determinato soggetto operata da un "terzo qualificato", della generazione della firma digitale all'interno di un dispositivo sicuro che contiene e custodisce anche la chiave privata, assicurandone la segretezza; del rispetto di determinate procedure e di particolari standard tecnici di sicurezza. Cammarata M., *Firme elettroniche, problemi normativi del documento informatico*, Monti & Ambrosini ed., 2007, p 32 e ss.

[53] Vale a dire l'effetto di fare proprio del sottoscrittore il contenuto del documento. Si veda Carnelutti F., "*Studi sulla sottoscrizione*", in *Riv. Dir. Comm.*, 1929, I. p. 526.

[54] Il cui art. 1 identifica le seguenti tipologie di firme elettroniche: 1) la firma elettronica "semplice", la cui definizione viene mutuata dal D. Lgs. n. 10/2002; 2) la "firma elettronica avanzata ai sensi dell'art. 2, co. 1, lett. g" del D. Lgs. n. 10/2002; 3) la "firma elettronica qualificata" di cui all'art. 1, lett. e, per tale dovendosi intendere "la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma"; 4) la "firma digitale", la cui descrizione è rimasta sostanzialmente invariata nel D. Lgs. n. 82/2005.

[55] Quest'ultimo passaggio è stato così modificato dal D. Lgs. n. 159/2006 allo scopo di inserire una traduzione più corretta della direttiva comunitaria.

sostituzione del precedente termine "autenticazione", compiuta con lo scopo di evitare confusioni con l'omonima espressione usata in ambito notarile e di sottolineare che la firma elettronica "semplice" ha lo scopo di indicare l'identità del soggetto[56], ha portato però a configurare la *electronic signature* come una *entity authentication*[57] e quindi una "firma debole", anziché strumento di validazione dei dati.

Il legislatore italiano contribuisce a complicare ulteriormente questo quadro omettendo di introdurre nel C.A.D. la *firma elettronica cd. avanzata* e inserendo comunque, all'art. 1 lett. s, la *firma digitale*, configurata come "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, 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"[58].

Alla luce delle considerazioni effettuate finora, appare chiaro che non esistendo, allo stato attuale delle conoscenze, dei *codes* diversi dalla coppia asimmetrica, la *advanced electronic signature* con certificato qualificato e dispositivo sicuro, di cui all'art. 5 della direttiva (o nella traduzione italiana "firma elettronica qualificata") finisca per corrispondere nella sostanza alla firma digitale[59].

Al termine di questo *excursus* sugli orientamenti dottrinali in merito alle cosiddette "diverse tipologie di firme elettroniche", può evidenziarsi una prevalenza dell'orientamento che tende a ritenere necessaria una correzione delle definizioni del C.A.D.[60], assieme ad una contestuale revisione della terminologia adottata nel contesto normativo, in modo da porre fine alle incertezze interpretative ed eliminare uno dei tanti ostacoli che impediscono alla firma digitale di diffondersi.

Quello che si farà nel capitolo seguente è esaminare le nuove regole tecniche recentemente approvate in materia di generazione, apposizione, verifica delle firme digitali e validazione temporale dei documenti informatici.

---

[56] Al riguardo la dottrina maggioritaria ha sempre sostenuto che intento del legislatore comunitario fosse quello di conferire dignità giuridica a molti processi di identificazione utilizzati nel commercio elettronico (Cuniberti, Lisi, Sirotti, Gaudenti).

[57] Osserva l'autore come *authentication* non si può tradurre con il termine "autenticazione", perché nel nostro ordinamento questa indica l'attestazione da parte del pubblico ufficiale che la sottoscrizione è apposta in sua presenza, essendo suo dovere di accertare l'identità della persona che sottoscrive (art. 2703 c.c.). L'espressione inglese, invece, può far riferimento sia alla validazione dei dati che alla validazione dell'identità. Cammarata M., *Firme elettroniche, problemi normativi del documento informatico*, Monti & Ambrosini ed., 2007, p 52 e ss.

[58]Con ciò si intende che la firma digitale è un specie del genus "firma elettronica qualificata". Ne deriva che attualmente l'unica firma elettronica qualificata esistente in Italia è la firma digitale. La definizione di "firma elettronica avanzata" era stata inserita all'epoca semplicemente per uniformarsi alla direttiva 1999/93 CE che la riportava. Nel CAD però si è deciso di toglierla, così di fatto eliminandola dal panorama normativo, preso atto dell'inesistenza nella realtà di un genere di firma elettronica avanzata diverso dalla firma digitale. Al momento, dunque, l'unica tipologia di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la generazione della firma è la firma digitale.

[59] Non può negarsi, infatti, che anche la firma elettronica qualificata consenta 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.

[60] Viste le considerazioni appena compiute, parlare di diverse tipologie di firme pensando alla firma elettronica qualificata, firma elettronica avanzata e firma digitale, potrebbe essere fuorviante.

2. Il funzionamento della firma digitale: le nuove regole tecniche

2.1 I riferimenti esistenti e il D.P.C.M. 30 marzo 2009

Il D. Lgs. n. 10/02 di recepimento della direttiva europea prevedeva, oltre alla modifica di alcuni articoli del T.U.D.A. esaminata nel capitolo precedente, la necessaria adozione di un regolamento per coordinare le disposizioni del T.U. con quelle del decreto legislativo stesso. Il regolamento venne approvato con D.P.R. n. 137/03, che modificò a sua volta il suddetto T.U. e portò all'emanazione, con D.P.C.M. 13 gennaio 2004, di nuove regole tecniche, volte ad aggiornare e a sostituire quelle del D.P.C.M. 8 febbraio 1999.

È prevista a breve l'emanazione di una serie di decreti ministeriali recanti ciascuno nuove regole tecniche, vista l'eterogeneità e la molteplicità degli argomenti disciplinati.

Nel momento in cui si scrive si è assistito all'emanazione del D.P.C.M. 30 marzo 2009 (pubblicato in G.U. n. 129 del 6 giugno2009) rubricato "*regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici*"[61]. Il decreto in questione, che è entrato in vigore il 3 dicembre 2009 [62] ed ha abrogato, sostituendola, la precedente regolamentazione tecnica datata 13 gennaio 2004, rappresenta il punto di riferimento tecnico principale in materia di firma digitale.

Queste nuove regole modernizzano il sistema della firma digitale, introducendo, in particolare, importanti novità in materia di conservazione delle chiavi e di validità nel tempo della marca temporale e della firma.

In questo capitolo si metterà a confronto la nuova regolamentazione tecnica con quella precedente con riferimento al processo di firma e alle vicende successive, allo scopo di evidenziarne le differenze e i punti salienti.

Il D.P.C.M. dispone la sostituzione dei riferimenti al D.P.R. n.445/2000 con quelli contenuti nel C.A.D. in materia di definizioni generali[63], mentre tralascia le definizioni delle regole tecnologiche[64],

---

[61] Lo stesso D.P.C.M. prevede l'abrogazione della circolare A.I.P.A. n. 24/2000 e delle Deliberazioni C.N.I.P.A. n. 4/2005 e n. 34/2006. Il procedimento di formazione delle regole tecniche generalmente proviene da un'istruttoria che opera il C.N.I.P.A., pur essendo le stesse adottate da organi politici e contenute in un D.P.C.M..

[62] Vale a dire decorsi centottanta giorni (sei mesi) dalla data di pubblicazione nella Gazzetta Ufficiale. In tal modo ne risulterà indiscutibile l'efficacia vincolante *erga omnes*, si tratti di pubbliche amministrazioni o di soggetti privati. Torsello M., Minerva M., *Il problema delle fonti* , in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 635.

[63] Quali, ad esempio, quelle di chiavi, documento informatico, autenticazione informatica, validazione temporale ecc..

[64] Ci si riferisce agli algoritmi usati, alle funzioni di *hash*, ai formati, alle caratteristiche delle chiavi utilizzate e dei certificati qualificati, agli elementi distintivi delle firme digitali e delle marche temporali, ecc..

demandandole a Deliberazioni del C.N.I.P.A., data la tecnicità della materia e la necessità di intervenire tempestivamente per introdurre quelle correzioni che dovessero essere richieste da improvvise evoluzioni tecnologiche[65]. Lo stesso art. 71 del C.A.D., al quale rinviano le singole discipline degli istituti I.C.T. (quali la firma digitale o la posta elettronica certificata) indica le fonti secondarie demandate ad adottare le regole tecniche in materia e le relative procedure[66].

Questo settore non si presta, dunque, all'approvazione parlamentare, caratterizzata da un *iter* normativo troppo lento che mal si concilia con i frequenti aggiornamenti propri dei contenuti tecnici. Si ravvisa, di conseguenza, la tendenza del Parlamento a spogliarsi della funzione legislativa e a delegare tale potestà all'autorità amministrativa.

La dottrina ha ritenuto opportuna, per gli stessi motivi, la prevalenza del potere del Governo o dei suoi componenti nella predisposizione delle regole tecniche, sconsigliando un intervento del Parlamento, privo di enti specialistici e strumenti tecnici per svolgere questo compito[67].

Parere opposto è stato quello manifestato dal Consiglio di Stato[68], secondo il quale le disposizioni integrative dell'art. 71 «*si configurano come norme generali, applicabili a tutte le pubbliche amministrazioni che incidono sui procedimenti amministrativi e sulle posizioni soggettive dei cittadini e delle imprese*» e che devono trovare, dunque, necessaria collocazione in «*una fonte normativa di rango primario*» [69].

La scelta privilegiata resta, comunque, quella di affidare la redazione della disciplina pubblica con contenuto tecnico al Governo e preferibilmente ai singoli Ministri, essendo questi ultimi dotati di una preparazione tecnica specifica nel ramo di propria competenza, e quindi in grado di redigere la regola tecnica in maniera più consapevole e approfondita di quanto possa fare l'organo legislativo.

Tra l'altro la legge è una fonte sconsigliata per adottare le regole tecniche, sia perché, come detto, nel caso di mutamento delle conoscenze tecnico-scientifiche, per modificarla si dovrebbe

[65] Tali modifiche, infatti, non potrebbero attendere i tempi necessari per l'emanazione e l'entrata in vigore di un nuovo decreto. Si pensi ad esempio alla sopravvenuta esigenza, per ragioni di sicurezza, di modificare la lunghezza delle chiavi di sottoscrizione (attualmente di 1024 *bit*).

[66] Tale articolo richiede al 1° co. che l'adozione delle regole tecniche, seppur prodotte da enti strumentali come il C.N.I.P.A.,debba avvenire con lo strumento del D.P.C.M. o con decreto del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate nel Codice. La procedura prevede altresì, oltre al parere della Conf. Unificata e del Garante per la privacy, l'acquisizione del parere tecnico obbligatorio del C.N.I.P.A.. Da ciò si ricava che le P.A., per applicare le tecnologie informatiche e telematiche ai loro procedimenti, dovranno necessariamente far ricorso alle citate regole tecniche.

[67] Arbia S., *La sicurezza dei dati*, in Quaranta M. (a cura di), *Il Codice della pubblica amministrazione digitale: commento ragionato al Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche*, Napoli, 2006, pp. 285 ss.

[68] *Consiglio di Stato, Parere n. 11995/05*; reso sullo schema di D. Lgs. contenente il C.A.D..

[69] Sul punto è intervenuta in passato anche la Corte dei Conti che, reputando il D.P.C.M. dell'8 febbraio 1999 non assoggettabile a registrazione, l'ha restituito. Sembra, dunque, che la Corte abbia aderito a quella tesi che non riconosce natura regolamentare al decreto in esame, trattandosi di statuizioni conseguenti a valutazioni di stretta discrezionalità tecnica, meramente applicative dei precetti contenuti nelle norme primarie e prive, pertanto, della idoneità ad innovare il sistema normativo vigente. Torsello M., Minerva M., *Il problema delle fonti* , in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 635.

adottare un'altra legge e quindi avviare un procedimento lungo e complesso, sia perché si verrebbe a produrre una scissione tra chi appare come l'autore dell'atto e chi l'ha realmente posto in essere, con inevitabili problemi in relazione alla permeabilità degli interessi all'interno del Parlamento[70].

Dall'indagine compiuta appare chiaro che le regole tecniche possono concretizzarsi in qualsiasi atto fonte del nostro ordinamento. La stessa normativa comunitaria, nell'illustrarle, vi include le disposizione legislative, regolamentari o amministrative, dotate di un contenuto tecnico-specialistico, cioè che mutuano al loro interno acquisizioni derivanti dalle scienze [71]. Ne consegue che, nella gerarchia delle fonti del diritto, esse si collocheranno al medesimo livello in cui generalmente si pongono le fonti da cui sono prodotte[72].

2.2 I presupposti di affidabilità della firma digitale

2.2.1 Il certificato qualificato ed il ruolo del Certificatore

Il legislatore italiano aveva compreso sin dal 1997 che per garantire la piena validità del documento informatico e l'affidabilità della firma digitale fosse necessario intervenire non solo sulla sicurezza delle tecnologie, ma soprattutto sulla serietà nella gestione dell'intero apparato. A tale scopo ha scelto il sistema che offre ancora oggi le maggiori garanzie di affidabilità sia dal punto di vista tecnologico che giuridico. Si tratta del sistema basato sull'infrastruttura a chiave pubblica o P.K.I.[73](*Public Key Infrastructure*), che resta l'unico capace di assicurare l'affidabilità, l'inalterabilità e la non ripudiabilità del documento informatico[74.]

Esso si avvale, innanzitutto, dello strumento del certificato qualificato, vale a dire del documento informatico che collega i dati utilizzati per verificare la firma elettronica al titolare, confermando così l'identità del titolare stesso. Viene definito qualificato essendo conforme ai requisiti fissati dall'allegato I della Dir. 1999/93/CE ed essendo emesso da un certificatore che risponde ai

[70] Dietro lo schermo della regola oggettiva di fatto si incide sul mercato, "*ci sono effetti che si producono per il solo fatto che si sceglie di ricorrere a una determinata tecnologia*", Rodotà, *Tecnopolitica, La democrazia delle nuove tecnologie della comunicazione*, La Terza 1997, p. 28.

[71] "*Costituiscono in ogni caso regole tecniche: 1) le disposizioni legislative, regolamentari o amministrative che fanno riferimento diretto ovvero indiretto, attraverso codici professionali o di buona prassi, a specifiche tecniche o ad altri requisiti o a regole relative ai servizi e la cui osservanza conferisce una presunzione di conformità alle prescrizioni fissate dalle suddette disposizioni legislative, regolamentari o amministrative;…".*Questa definizione, presente nel testo della direttiva comunitaria 1998/34/CE, è stata recepita nel nostro ordinamento dal D. Lgs. n. 427/00 ed è quindi valida e obbligatoria.

[72] Iannuzzi A., *Caratterizzazioni della normazione tecnica nell'ordinamento italiano. Il campo di analisi e di verifica della materia ambientale,* in *http://www.associazionedeicostituzionalisti.it/materiali/anticipazioni/caratterizzazioni/index.html* , 30 ottobre 2006.

[73] Termine con il quale si fa riferimento ad un insieme di *standard, software* e procedure allo scopo di realizzare validi sistemi di autenticazione.

[74] Maccarone E., *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici,* a cura di Bianca, in *Nuove Leggi civ. comm.*, 2000, III-IV, 661.

requisiti fissati dall'allegato II della direttiva medesima[75] e dunque "accreditato", cioè capace di rilasciare i "certificati qualificati"[76] e di garantire controlli e sicurezza maggiore nel meccanismo di sottoscrizione elettronica[77].

Va ricordato che, ai sensi del D.P.R. n. 137/03 e successivamente del C.A.D., l'attività di "certificatore" può essere esercitata non solo da una persona giuridica, ma anche da una persona fisica. Ciò si desume sia dalla definizione di certificatore, la quale lo configura come un "soggetto che presta i servizi di certificazione", sia nell'ambito dei requisiti di onorabilità, dal riferimento a "certificatori o, se persone giuridiche, i loro legali rappresentanti"[78]. La dottrina ha sollevato seri dubbi in merito alla decisione di affidare il servizio di certificazione a persone fisiche, trattandosi di un'attività delicata che presuppone garanzie di affidabilità e solvibilità in caso di responsabilità, nonché organizzazione e strutture complesse. Tale scelta trova fondamento nella necessità di conformarsi alla previsione comunitaria delle firme elettroniche semplici basate su certificati elettronici non qualificati, che resta l'unica ipotesi in cui è consentito ad una persona fisica di svolgere attività di certificazione[79].

Il certificatore, che dunque si caratterizza per la sua terzietà ed imparzialità rispetto agli utenti, ha il compito di identificare con certezza l'identità del richiedente la coppia di chiavi, rilasciare e rendere pubblico il certificato[80] in conformità alle regole tecniche in vigore e al D. Lgs. n.196/03[81]; pubblicare e tenere aggiornato l'elenco delle chiavi pubbliche (corrispondenti a quelle private) e dei relativi certificati, nonché le vicende relative alla coppia di chiavi; provvedere tempestivamente alla revoca o sospensione delle chiavi nei casi previsti dall'art. 32 lett. g del C.A.D.[82].

Si comprende pertanto l'importanza del ruolo svolto dal certificatore attraverso il procedimento di accertamento dell'identità: questa fase preliminare, se compiuta in modo corretto, è in grado di

[75] Le cui disposizioni di recepimento si ritrovano nel C.A.D. rispettivamente agli artt. 28 e 29.

[76] Occorre precisare che il certificatore accreditato si differenzia da quello qualificato grazie alla sussistenza di un preventivo riconoscimento da parte del C.N.I.P.A., che attesta la presenza di tutti i requisiti indicati dall'art. 29 del C.A.D., attribuendo così alla certificazione un più elevato livello di qualità e sicurezza.

[77] Inoltre l'art. 34 del C.A.D. aggiunge che anche le pubbliche amministrazioni, ai fini della sottoscrizione di documenti informatici di rilevanza esterna, possono rilasciare certificati qualificati esclusivamente nei confronti dei propri organi o uffici, nonché di categorie di terzi, ma i certificati rilasciati a questi ultimi possono essere utilizzati solo nei rapporti con l'Amministrazione certificante. Per svolgere la suddetta attività le P.A. hanno l'obbligo di accreditarsi presso il C.N.I.P.A., che svolge le funzioni di garante dei requisiti prescritti dalla legge per l'esercizio dell'attività di certificazione e gestisce il relativo elenco pubblico dei certificatori. Per quanto riguarda invece la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna le P.A. possono darsi, nella propria autonomia organizzativa, una disciplina diversa da quella contenuta nelle regole tecniche vigenti.

[78] Entrambe confluite rispettivamente nell'art. 1 lett. g e nell'art. 26 co. 1° del C.A.D.. Quest'ultimo, in particolare, abilita il certificatore semplice a svolgere liberamente la propria attività, senza nessun tipo di autorizzazione, essendo richiesto a tal fine il solo requisito di onorabilità.

[79] Sorrentino F., *La disciplina sulle firme elettroniche: ultimo tassello?*, in *Nuove Leggi Civ. Comm.*, 2003, 4-5, 809.

[80] In ogni caso il certificatore conserva presso di sè una copia del certificato emesso.

[81] Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

[82] In caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all' articolo 71.

intercettare una possibile sostituzione di persona e dunque fornire agli utenti sufficienti garanzie sulla provenienza e autenticità di un documento informatico, in modo da accrescerne il valore probatorio [83].

Le nuove regole tecniche hanno ampliato il disposto dell'art. 14 prevedendo altresì che il certificatore assicuri la consegna al legittimo titolare delle chiavi da lui generate; mentre nell'ipotesi di chiavi non generate dal certificatore, provveda a verificare il possesso della chiave privata da parte del titolare e il corretto funzionamento della coppia di chiavi[84]. Si aggiunge poi un'ulteriore precisazione sul termine del periodo di validità del certificato qualificato, il quale deve essere anteriore rispetto al termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità. In tal modo si è voluto evitare il paradosso di un certificato di sottoscrizione con validità superiore al certificato di certificazione utilizzato dal certificatore per sottoscriverlo[85]. Nel successivo articolo 15 si ribadisce la competenza del certificatore a stabilire il periodo di validità del certificato[86], ma si accresce l'autorità del C.N.I.P.A., a cui spetta nel contempo determinare il periodo massimo in considerazione della robustezza delle tecnologie in uso. Infine si precisa che il certificatore debba custodire tutte le informazioni relative al certificato qualificato per almeno venti anni dal momento della sua emissione.

Il certificato qualificato contiene i seguenti elementi: codice identificativo del titolare presso il certificatore; le sue generalità e quelle del certificatore; la tipologia della coppia di chiavi in base all'uso cui sono destinate; chiave pubblica, ossia i dati per la verifica della firma[87]; la data di scadenza ed eventuali limitazioni d'uso o negoziali.

In particolare la nuova versione dell'art. 15 delle regole tecniche del 2009 prevede la possibilità di inserire le qualifiche del titolare all'interno del certificato, come già previsto dalla Deliberazione C.N.I.P.A. n. 4/2005, che viene conseguentemente abrogata[88].

Il certificato, infine, è firmato digitalmente dal certificatore, in modo che sia possibile verificare l'autenticità dello stesso[89]. A tal fine il certificatore genera, per ciascuna chiave di certificazione, un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce[90].

---

[83] Il legislatore italiano ha posto in capo al certificatore tutte le responsabilità derivanti dall'esercizio dell'attività di certificazione, con l'intento di offrire agli utenti una maggiore tutela. Ciò significa che è responsabile, se non prova di aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento sul certificato qualificato da lui rilasciato (art. 30 co. 1 C.A.D.).

[84] Va tenuto presente che un certificato non qualificato può essere anche autogenerato da un utente, previa richiesta ad un gestore che provvede ad inviarlo per *e-mail*, senza però che si proceda ad un'identificazione sicura del richiedente.

[85] Il certificatore utilizza la propria chiave privata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare; C.N.I.P.A. – Ufficio Sicurezza, *Guida alla Firma Digitale* , in *http://www.cnipa.gov.i t/html/docs/GuidaFirmaDigitale2009_a.pdf*, Aprile 2009.

[86] Naturalmente il certificatore ha tutto l'interesse economico a fissare brevi termini di validità, perché la riemissione del certificato, giustificata da esigenze di sicurezza, è solitamente legata ad un pagamento.

[87] Cioè dati peculiari come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica, corrispondenti ai dati per la creazione della stessa in possesso del titolare (art. 28 co. 1 lett. e C.A.D.).

[88] Dunque, seppur il titolare del certificato deve essere una persona fisica, all'interno del certificato può essere indicata anche l'organizzazione di appartenenza e il titolo o il ruolo ricoperto all'interno della stessa, purché ci sia stata una richiesta da parte dell'organizzazione in tal senso.

Occorre precisare che la firma generata attraverso un dispositivo sicuro che custodisce al suo interno la chiave privata e dotata di una certificazione emessa da un certificatore non qualificato[91], resta pur sempre una firma elettronica "debole", che non garantisce l'identità del firmatario, in quanto mancante del certificato qualificato e quindi della chiave privata di un soggetto terzo che associ in maniera sicura il certificato alla persona[92].

Viceversa la firma digitale fornisce la certezza della paternità del documento, e quindi della provenienza, grazie alla procedura di certificazione, che attesta l'attribuzione delle chiavi di sottoscrizione a un determinato soggetto, il solo a poterle usare per mezzo del possesso esclusivo del dispositivo di firma.

In conclusione si può affermare che, grazie alla procedura di certificazione, è possibile garantire l'autenticità delle chiavi, la corrispondenza della chiave pubblica con il suo titolare e di conseguenza dimostrare la validità di una firma digitale e la sua imputabilità ad un determinato soggetto.

[89] Vale a dire, più esattamente, con firma elettronica qualificata, idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo (art. 28 co. 1 lett. g C.A.D.). Al riguardo, una precisazione da fare è che in Italia i termini finora usati di firma digitale e di firma elettronica qualificata si riferiscono in realtà solo alla firma basata sul certificato cd. qualificato. Il certificato qualificato può essere rilasciato solo ad una persona fisica, non giuridica (dovrà recare il nome e cognome di una persona fisica, non di un'azienda). Quindi, per correttezza, quando si parla di firma "digitale" del certificatore, si dovrebbe usare l'espressione di "firma elettronica", proprio perché il certificato non è a nome di una persona fisica, ma di una persona giuridica. Il fatto che il certificato non sia qualificato non è indice di minor sicurezza, ma dipende appunto dalla mancanza del nome, cognome, codice fiscale di una persona fisica e dall'indicazione della denominazione di una persona giuridica; Arbia S., *Ufficio Sicurezza* – C.N.I.P.A..

[90] Ai sensi dell'art. 13 del D.P.C.M. 30 marzo 2009, rimasto invariato rispetto al medesimo art. del D.P.C.M. 13 gennaio 2004. Ciò significa che il certificatore usa la propria chiave privata per sottoscrivere il certificato ed in questo modo sottoscrive sostanzialmente la connessione fra il possessore di una chiave pubblica ed i suoi dati anagrafici. Questo consente al destinatario, una volta pervenuta la busta crittografica (cioè il *file* contenente il documento informatico e le informazioni relative alla firma, tra cui in particolare l'*hash* cifrato con la chiave privata ed il certificato comprensivo della chiave pubblica), di verificare, per mezzo dell'apposito *software*, che quell'*hash* sia stato cifrato con la chiave privata corrispondente alla chiave pubblica posta all'interno del certificato e dichiarata appartenente a quel mittente da parte del certificatore. A tal fine il *software* prende la chiave pubblica all'interno di quel certificato, la usa per decifrare l'*hash* (a sua volta cifrato con la corrispondente chiave privata del mittente), ricalcola l'*hash* del documento e li confronta, se sono uguali si ha la garanzia dell'integrità del testo e della sua provenienza da chi appare come mittente.

[91] Si pensi alla certificazione interna ad un'azienda.

[92] Va ricordato che tale firma, pur essendo definita debole, può essere allo stesso modo sicura. Essa, infatti, garantisce l'integrità dei dati, avvalendosi della funzione di *hash* e di un sistema di chiavi asimmetriche a coppia. Ciò che la differenzia, come si vedrà meglio più avanti, è il valore probatorio. Infatti, il C.A.D. all'art. 21, attribuisce valore giuridico al documento sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, mentre dà valore probatorio variabile ad altre tipologie di firme elettroniche eventualmente avanzate. Ciò vuol dire che il documento sottoscritto con firma digitale dovrà essere acquisito dal giudice quale prova, al contrario quello recante una firma elettronica, che potrebbe essere identica sotto il profilo della sicurezza, dovrà essere valutato dal giudice.

2.2.2 Il dispositivo di firma

Il dispositivo sicuro per la creazione della firma rappresenta, accanto al certificato qualificato, il secondo presupposto di affidabilità della firma digitale o di altro tipo di firma elettronica avanzata, essendo congegnato per impedire l'intercettazione della chiave privata utilizzata.

Le nuove regole tecniche ne richiedono, similmente al passato, la conformità alle norme generalmente riconosciute a livello internazionale (art. 3). Viene precisato che la certificazione di sicurezza deve osservare criteri non inferiori ai Profili di Protezione fissati dalla CE e dal C.A.D.[93]. La disciplina resta immutata anche con riguardo alla fase di attivazione, precedente la generazione della firma, che richiede l'azione esclusiva del titolare attraverso l'inserimento di codici personali. A tale proposito il C.A.D. aggiunge all'art. 35 che i dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata sia riservata; che non possa essere derivata e che la relativa firma sia protetta da contraffazioni; che possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi. A tal fine le chiavi devono essere custodite dal titolare in un dispositivo sicuro protetto da *password*, quale può essere una *smart-card*, una chiavetta *usb*, un *token* ed anche dispositivi di firma particolari denominati HSM.

La novità riguarda l'incremento dei poteri del C.N.I.P.A., a cui è stata affidata la verifica dell'adeguatezza tecnologica delle modalità di autenticazione in relazione ai dispositivi di firma usati (art. 9 co. 3).

Il D.P.R. n. 137/2003 definiva dispositivo per la creazione della firma "il programma informatico adeguatamente configurato (*software*) o l'apparato strumentale (*hardware*) usati per la creazione della firma elettronica" e dispositivo sicuro per la creazione della firma "*l'apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'art. 10 D. Lgs. 23 gennaio 2002 n. 10*"[94]. Ciò significa che "i criteri per la creazione delle chiavi asimmetriche (privata e pubblica della firma digitale) come pure di altri sistemi di firme elettroniche avanzate e, quindi, gli algoritmi e le procedure necessarie per la loro applicazione, non possono essere lasciati alla discrezionalità di ciascun firmatario…ma devono essere programmate in un *software* immodificabile, autorizzato e controllato dall'Autorità, racchiuso in una *smart-card* (normalmente costituita da una scheda di plastica contenente microcircuiti e *chips* e, quindi, un vero e proprio *microcomputer*), la cui introduzione nel computer del firmatario sia necessaria e sufficiente per generare, con criteri di casualità, una chiave segreta con cui criptare i messaggi, e una chiave pubblica correlata con cui

[93] Ci si riferisce altresì alla necessaria rispondenza ai requisiti prescritti dall'allegato III della direttiva europea 1999/93/CE ed allo schema nazionale per la valutazione e certificazione di sicurezza ex art. 35 del C.A.D..

[94] Tale definizione di dispositivo sicuro viene richiamata nell'art. 1 lett. r del CAD con riferimento alla firma elettronica qualificata. In tale contesto si parla di apparato strumentale per precisare che un eventuale *software* situato su un *server* non sarà mai un dispositivo sicuro per la creazione della firma, perché mancante dei requisiti per un adeguato livello di certificazione. Non è invece presente nel C.A.D. la definizione di dispositivo, che va inteso pur sempre come apparato *software* ed *hardware* usato per la creazione della firma elettronica.

decifrarli[95]". La *smart-card*, dunque, è stata così strutturata anche per facilitare e diffondere l'utilizzo della firma digitale, senza dover ricordare tutte le fasi della procedura a ciò necessaria[96].

Se dunque, da un lato si promuove l'uso della firma digitale garantendo alti livelli di sicurezza tecnica, dall'altro si continua a dubitare della sua sicurezza legale. La dottrina[97], infatti, ha posto l'attenzione sulla difficoltà di assicurare con sicurezza il possesso e quindi l'uso del dispositivo di firma da parte del titolare apparente, sebbene questo si presuma in base all'art. 21, co. 2° del C.A.D..

Accade, ad esempio, che i certificatori consegnino ai responsabili di azienda dispositivi di firma per sottoscrivere la documentazione amministrativa e contabile, ma costoro diano in realtà tali dispositivi (ed i relativi PIN) ad intermediari, suggerendo in tal modo la presunzione del possesso in capo a questi ultimi. In ogni caso sarà il titolare del dispositivo a rispondere dei comportamenti posti in essere dall'intermediario o dal terzo affidatario del dispositivo stesso.

Allo scopo di porre fine a simili comportamenti ed aumentare la fiducia nella firma digitale è stata introdotta una modifica all'art. 32, co. 1° del C.A.D., laddove si prevede, fra gli obblighi del titolare del certificato di firma, anche quello di utilizzare personalmente il dispositivo di firma. Ne deriva l'impossibilità di cedere ad altri il dispositivo di firma, pena responsabilità civili e penali.

2.2.3 Il sistema di crittografia a chiavi asimmetriche

La firma digitale costituisce diretta applicazione della tecnologia crittografica asimmetrica. Il sistema di crittografia a chiavi asimmetriche, pur non rappresentando un presupposto di affidabilità della sola firma digitale, ma più in generale delle firme elettroniche, è stato richiamato in questo punto della trattazione per sottolineare come esso abbia conferito alla firma digitale e di riflesso al documento elettronico, sicurezza ed efficacia giuridica pari a quelle della sottoscrizione autografa. Attraverso la firma digitale, infatti, è stato possibile attribuire il valore di piena prova alla documentazione prodotta, gestita e trasmessa attraverso l'uso del *computer*, prescindendo dalla necessità della relativa stampa, e quindi della relativa sottoscrizione.

Dunque, grazie all'impiego della suddetta tecnica, si è garantita la genuinità, la provenienza e non ripudiabilità del documento[98]. Sulla base di queste considerazioni si può

[95] Borruso R., *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (D. Lgs. 23 gennaio 2002 n. 10, D.P.R. 7 aprile 2003 n. 137 e L. 29 luglio 2003 n. 229*, in *Giust. Civ.*, 2004, n. 3, p. 155.

[96] È sufficiente, infatti, inserire la *smart-card* nel proprio *computer*, selezionare il documento che si desidera firmare e confermare la volontà di generare la firma affinché la procedura possa considerarsi perfezionata. Si tratta, come si vede, dell'apposizione di un sigillo ad un certo testo e non di una sottoscrizione nel senso comune del termine.

[97] Buonuomo G., *Effetti probatori: si torna al processo civile*, in *http: //www.interlex.it/docdigit/buonomo13.htm*, 20-01-2005.

[98] Quest'ultima si estrinseca nell'impossibilità di disconoscerlo come proprio una volta sottoscritto, nonché, con l'ausilio della Posta Elettronica Certificata, nell'impossibilità per il destinatario di negare di averlo ricevuto.

affermare che la sicurezza della firma digitale è intrinseca al sistema crittografico ad essa sotteso.

La tecnica di crittografia a "*chiavi asimmetriche*" viene così chiamata perché si avvale di due chiavi diverse, una per cifrare e l'altra per decifrare il contenuto di un documento, in modo da renderlo nascosto a chi non possiede la chiave per decifrarlo[99].

Le chiavi sono degli insiemi di numeri e lettere[100], che vengono generate casualmente dal *computer* attraverso degli algoritmi, cioè delle procedure di calcolo inserite in un programma specifico, per essere collegati entrambi al medesimo utente. Le due chiavi sono univocamente correlate, per cui ad una chiave privata corrisponde una ed una sola chiave pubblica; complementari, nel senso che il documento cifrato con una può essere decodificato solo usando l'altra[101]; e indipendenti perchè la conoscenza della chiave pubblica non consente di risalire alla corrispondente chiave privata.

Dunque, essendo infinitesimali le possibilità di corrispondenza della chiave di una coppia con quella di un'altra coppia, si può ritenere il sistema assolutamente sicuro.

Il titolare della coppia di chiavi, essendo per definizione l'esclusivo utilizzatore della chiave privata, ha l'onere di mantenerla segreta[102] e comunicare quella pubblica, che servirà per verificare la firma, all'Autorità di Certificazione; la quale, una volta accertata l'identità del richiedente, emetterà un certificato ad essa associato, contenente la suddetta chiave pubblica [103]. Tale sistema, come si vede, fonda l'imputazione del documento sull'esclusività dell'uso del mezzo, e non sull'univocità della calligrafia di firma.

La chiave privata, dunque, assieme all'apposito *software*, consente al possessore di apporre la firma digitale sul documento informatico. Va precisato, però, che il processo di firma di per sè non consente di ottenere segretezza perché oggetto della cifratura è il risultato dell'algoritmo di hash e non il documento, che resta in chiaro [104].

La crittografia si avvale di vari metodi cifratura, creati per rispondere a diverse esigenze[105]. In primo luogo quella di attestare l'autenticità del documento e la possibilità di collegarne il contenuto al suo autore. In tal caso questi dovrà cifrare il documento con la propria

[99] A differenza della crittografia simmetrica che si avvale di una sola chiave segreta che serve sia per criptare che per decriptare il documento e che deve essere mantenuta segreta da entrambe le parti, per il successo del metodo. Questa tecnica risulta però svantaggiosa in quanto la suddetta chiave può essere utilizzata per lo scambio di messaggi fra una sola coppia di utenti e nel caso di comunicazione con diversi soggetti è necessario adottare chiavi diverse per ognuno di essi. Inoltre non v'è sicurezza dell'autenticità e dell'integrità del documento perché le parti condividono la chiave di criptazione (la sicurezza si può avere nei confronti dei terzi, non tra le parti).

[100] Stringhe composte da 128 caratteri alfanumerici.

[101] Ciò significa, in altre parole che, se si cifra un documento con la chiave privata occorrerà decifrarlo con la chiave pubblica; viceversa se si cifra con la chiave pubblica si dovrà decifrare con quella privata.

[102] In realtà neanche il titolare conosce la sua chiave privata, data la sua estensione, la custodisce in un dispositivo (in genere una *smart-card*) e la procedura si avvia solo quando si inserisce il dispositivo nel *computer*.

[103] Tale certificato dovrà essere allegato ogni volta in cui il soggetto appone la propria firma digitale.

[104] La chiave, tramite l'applicazione dell'algoritmo di cifratura, trasforma un testo in chiaro in un testo cifrato e dunque rappresenta il codice che consente di attivare l'algoritmo.

[105] Piccoli P., Zanolini G., *Il documento elettronico e la firma digitale*, in *Riv. Notariato.*, 2000, n. 4, p. 885 e ss.