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

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.

chiave privata, in modo tale che il destinatario lo possa decifrare con la corrispondente chiave pubblica del sottoscrittore. Se l'operazione di verifica ha esito positivo è assicurata l'integrità e la provenienza di un documento informatico poiché si presume che soltanto il legittimo titolare della chiave privata possa averla usata per cifrarlo. Questo sistema genera però un inconveniente: essendo la chiave pubblica per definizione conoscibile da chiunque, può accadere che, una volta ottenuta la disponibilità del documento, chiunque vi applichi la suddetta chiave ne possa leggere il contenuto. Pertanto, se si vuole assicurarne la segretezza, sarà necessario che l'autore cifri il documento con la chiave pubblica del destinatario, in modo che solo quest'ultimo ne potrà conoscere il contenuto decifrandolo con la propria chiave privata. Ciò va però a discapito dell'autenticità del documento, dal momento che chiunque può utilizzare la chiave pubblica del destinatario per eseguire la cifratura[106].

Per raggiungere congiuntamente le garanzie di paternità, integrità e segretezza ora esaminate, che caratterizzano una firma digitale, si dovrà ricorrere ad un terzo metodo di cifratura che si basa sull'uso combinato delle chiavi: il documento viene cifrato dal sottoscrittore sia con la propria chiave privata, per dare certezza al ricevente della provenienza, che con quella pubblica del destinatario, per dare segretezza al messaggio. Ne consegue che soltanto il destinatario potrà decodificare il testo facendo uso della sua chiave privata e, al tempo stesso assicurarsi dell'autenticità utilizzando la chiave pubblica del sottoscrittore[107].

Si osserva in dottrina come "*la sicurezza del sistema descritto consiste nel fatto che se la chiave pubblica non corrisponde a quella privata, ovvero se il messaggio è stato, anche in minima parte modificato, il messaggio stesso diviene indecifrabile, rendendo in tal modo manifesta l'apocrifia del messaggio o la sua alterazione*"[108].

Ne deriva che se il testo viene modificato anche in un solo particolare, la firma digitale ottenuta attraverso la sua compressione (*funzione di hash*) e la sua cifratura, pur con la chiave del medesimo autore, risulterà ogni volta diversa.

---

[106] Tale sistema è conforme al disposto del D.P.R. 513/97, laddove all'art. 1 si configura la chiave pubblica come l'elemento della coppia di chiavi asimmetriche con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi. In realtà quest'ultima parte è scomparsa nella definizione di chiave pubblica contenuta all'art. 1 lett. i del C.A.D.. Ciò è dipeso probabilmente dalla natura legislativa del C.A.D., che è stato strutturato in modo da contenere solo definizioni generali e non elementi tecnici. Quello della cifratura è per l'appunto un elemento tecnico che, pur essendo stato omesso, non esclude la validità dei molteplici usi della crittografia.

[107] Si richiede, dunque, l'ulteriore cifratura con la chiave pubblica del destinatario allo scopo di garantire la segretezza dei dati, in quanto l'oggetto firmato all'interno del dispositivo mantiene il testo in chiaro. Per questa ragione i certificatori normalmente forniscono i dispositivi di firma digitale con a bordo due certificati e due coppie di chiavi: un certificato e una coppia di chiavi vengono utilizzati esclusivamente per la firma digitale, il secondo certificato con la corrispondente ulteriore coppia di chiavi, distinta dalla prima, sono usati appunto per la crittografia e per l'autenticazione. In pratica il mittente, dopo aver sottoscritto il testo, chiede al destinatario il suo certificato di autenticazione e con la chiave pubblica inclusa al suo interno cifra il documento. Il destinatario, a sua volta, userà la chiave privata contenuta nel suo certificato di autenticazione, a bordo della *smart card*, per decifrare il documento e verificare la firma.

[108] Piccoli P., Zanolini G., *Il documento elettronico e la firma digitale*, in *Riv. Notariato.*, 2000, n. 4, p. 883.

Tale meccanismo consente pertanto di ottenere garanzie superiori rispetto a quelle fornite dalla sottoscrizione autografa. Oltre a svolgere una funzione indicativa, essendo possibile identificare con certezza l'autore del documento attraverso una associazione tecnica e giuridica tra la chiave privata e la chiave pubblica di cui è titolare; una funzione dichiarativa, poiché attraverso la firma digitale si approva il contenuto del documento e ci si assume la paternità delle dichiarazioni in esso rese [109] ed una funzione probatoria, assolta dalla firma digitale in unione al certificato relativo alla stessa[110], essa è in grado di garantire l'assenza di postume correzioni, cancellazioni o aggiunte.

Alla luce delle considerazioni effettuate finora appare chiaro che, eliminando quelle incertezze legate al riconoscimento dell'autografia e al timore che un testo abbia subito delle modifiche per opera altrui e senza autorizzazioni di sorta, la firma digitale potrà rilevarsi uno strumento idoneo a tutelare alcuni valori fondamentali dell'ordinamento ed a favorire lo sviluppo del commercio elettronico[111].

2.3 Le fasi del processo di firma

2.3.1 Generazione della coppia di chiavi

Dalla lettura delle nuove regole tecniche si osserva come la procedura prevista per la generazione della coppia di chiavi non abbia subito modificazioni. Vale la pena comunque soffermarsi sui tratti salienti per comprenderne il funzionamento.

Anzitutto va ricordato che esistono diverse tipologie di chiavi di creazione e verifica della firma; in particolare si distingue fra chiavi di sottoscrizione, certificazione e di marcatura temporale. Si tratta di chiavi basate sulla stessa tecnica informatica (sistema di cifratura delle chiavi asimmetriche), ma ciascuna coppia può essere utilizzata esclusivamente per le funzioni individuate per ciascuna tipologia (art. 4).

L'art. 5 richiede che il sistema di generazione garantisca, con riferimento alla coppia di chiavi, il rispetto dei relativi requisiti imposti dagli algoritmi di generazione e di verifica utilizzati; che gli algoritmi assicurino l'equiprobabilità di generazione di tutte le chiavi possibili, vale a dire lo stesso grado di probabilità di essere generate; che vi sia l'autenticazione informatica del soggetto che attiva

[109] Il documento potrebbe, infatti, essere stato redatto da altri ma é solo colui che lo sottoscrive che si assume la responsabilità delle dichiarazioni in esso contenute come manifestazione della propria volontà. In realtà, non si ha più paternità in senso stretto, bensì titolarità della firma. L'uso esclusivo della chiave privata sostituisce l'esclusività della grafia manuale.

[110] La funzione probatoria deriva dalla combinazione delle funzioni precedentemente analizzate: serve per provare l'autenticità del documento e cioè la provenienza delle dichiarazioni contenute nel documento da chi l'ha sottoscritto. In tal caso si può affermare che il documento ha valore probatorio.

[111] Basti pensare alla tutela della buona fede, alla lotta alle frodi e alla semplificazione dei negozi.

la procedura di generazione. La sostituzione dell'espressione "identificazione del soggetto" con quella di "autenticazione informatica" sembrerebbe volta a porre in risalto la capacità del *software* di garantire la sicurezza dell'accesso ad un sistema informatico, attraverso la verifica preliminare, o validazione, dell'identità di colui che chiede di essere abilitato alla generazione.

L'art. 6 opera una distinzione fra i soggetti abilitati a generare le coppie di chiavi in relazione alle diverse tipologie di chiavi. Si è detto pocanzi che sussistono chiavi di certificazione e di sottoscrizione. Le prime possono essere generate esclusivamente in presenza del responsabile del servizio. Le chiavi di sottoscrizione, invece, possono essere generate sia dal titolare che dal certificatore. Il titolare dovrà comunque generare le chiavi all'interno del dispositivo sicuro rilasciato o indicato dal certificatore a tal fine[112] e per mezzo di un apposito *software*.

Nel caso di generazione delle chiavi al di fuori del dispositivo di firma, e dunque su un sistema diverso da quello di generazione della chiave privata, il sistema dovrà essere tale da impedire, nel modo più assoluto, qualsiasi intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura; garantire il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui verrà utilizzata; essere esclusivamente dedicato all'attività di generazione ed adeguatamente protetto[113].

In ogni caso, prima di iniziare una procedura di generazione delle chiavi, deve verificarsi l'autenticità e l'integrità del *software* installato, l'assenza di programmi non previsti dalla procedura e di dati residuali provenienti dalla generazione di coppie di chiavi precedenti che possano inficiare l'equiprobabilità della generazione di quelle successive.

2.3.2 Conservazione delle chiavi e dei dati per la creazione della firma

Di seguito l'attenzione si concentra su uno dei cambiamenti più significativi operati dal decreto in esame, che trova il suo fulcro nella previsione dell'art. 7 avente ad oggetto, a seguito della modifica, non solo la conservazione delle chiavi, ma altresì quella dei "dati per la creazione della firma", vale a dire quegli elementi di sicurezza necessari per la generazione della firma (dunque chiave privata e P.I.N.).

Sebbene la legislazione in materia, dapprima il DPR n. 445/00 all'art. 28 co. 1° lett. g ed in seguito il C.A.D. all'art. 32 lett. f e k, proibisca che la chiave privata possa essere depositata presso il certificatore, sia pure in plico sigillato, tale ostacolo è stato aggirato grazie ad alcune varianti inserite nel nuovo D.P.C.M. 30 marzo 2009, a cui dovrà seguire necessariamente la modifica delle norme del C.A.D. ad esse collegate; in modo che l'interpretazione fornita da tali regole di rango inferiore, ma di maggiore specificità, possa assurgere ad un livello più alto ed acquisire così maggior valore giuridico.

[112] Tale dispositivo dovrà avere le caratteristiche ed i requisiti di sicurezza previsti dalla legge.
[113] Art. 8, D.P.C.M. 30 marzo 2009.

In primo luogo, per vincere il divieto posto dal C.A.D. in capo al certificatore circa i dati per la creazione della firma è stato necessario introdurne la definizione, come previsto dalla nuova lettera e dell'art. 1 del citato D.P.C.M.: "*l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica*". In tal modo si è colmata una lacuna presente nel C.A.D. che non fornisce alcuna precisazione in merito.

In secondo luogo, per superare il divieto posto dall'art. 7 delle regole tecniche del 2004 in capo al titolare della coppia di chiavi, è stata aggiunta al co. 3° la lett. d contenente l'inciso in base al quale questi "*mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma*". È sufficiente, dunque, che il titolare mantenga in modo esclusivo la conoscenza/disponibilità del P.I.N.-che rappresenta uno dei "dati per la creazione della firma"- in modo da rispettare il dettato delle regole tecniche.

A ciò si è aggiunta l'interpretazione evolutiva[114] dell'art. 32 lett. f del C.A.D. che, come detto, sancisce il divieto per il certificatore di rendersi depositario dei dati per la creazione della firma del titolare. Alla luce delle considerazioni effettuate, visto che "dati per la creazione della firma" sono l'insieme dei codici (chiave privata e P.I.N.) il certificatore non contravviene alla norma se si limita a detenere (che equivale a conservare e non a disporre) unicamente la chiave privata.

Va precisato, però, che tali dati vanno conservati su particolari dispositivi sicuri per la generazione della firma (*Hardware Security Module*[115]) situati presso la propria struttura, all'interno di locali adeguatamente protetti. Ciò non implica che il certificatore debba essere informato sugli atti o fatti oggetto della sottoscrizione, che restano nella conoscenza esclusiva del firmatario, assieme ad almeno uno dei dati per la creazione della firma.

La suddetta interpretazione trova fondamento altresì nell'art. 9 delle regole tecniche che al co. 2° richiede l'attivazione del dispositivo sicuro, prima della generazione della firma, per opera del solo titolare, attraverso codici personali; ed al successivo co. 3° fornisce un ulteriore garanzia di sicurezza prevedendo la valutazione del C.N.I.P.A. sull'adeguatezza tecnologica delle modalità di gestione dei codici personali, anche in relazione al dispositivo di firma utilizzato.

Secondo questa lettura della normativa indicata ufficialmente dal C.N.I.P.A.[116], così facendo si svincolerà l'uso della firma digitale alla disponibilità in locale[117] di un apposito applicativo, (ossia del *software* di firma, che potrà essere disponibile in rete) e di un apposito *hardware* (in altre parole potranno non essere più necessari dispositivi fisici quali il lettore e la connessa *smart card* o *token usb* che sia). Il che potrà aprire la strada alla cd. firma remota: ciò significa che, una volta selezionata tale opzione, l'*hash* creato in locale verrà inviato via *web* attraverso il *software* di firma[118].

---

[114] C.N.I.P.A. - *Ufficio Sicurezza*.

[115] Da ora: H.S.M..

[116] 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.

[117] Cioè sul proprio *personal computer*.

[118] In ogni caso la firma, con la relativa generazione dell'*hash*, possono essere effettuate interamente tramite un'applicazione *web*.

In pratica il *software*, non dialogando più con la *smart card*, si collegherà *on line* ai servizi forniti dal certificatore il quale, come detto, non potrà visualizzare il contenuto del documento[119]. A questo punto, per consentire la cifratura dell'*hash* con la chiave privata, saranno necessarie adeguate misure di autenticazione; in modo che solo il legittimo titolare di quella coppia di chiavi sia in grado di richiedere un'operazione di firma sull'H.S.M.. Occorrerà cioè, oltre al certificato, l'inserimento della *user id* dell'utente, del P.I.N. e di una *password* aggiuntiva generata dal *software* e valevole unicamente per quella firma, ragione per cui prende il nome di O.T.P. (*One time password*). Solo successivamente all'inserimento di questi codici sarà possibile firmare digitalmente il documento[120].

Tutto ciò è stato realizzabile grazie alla possibilità di variare i requisiti di sicurezza sulla base delle caratteristiche del certificato[121]: "se usiamo un certificato con forti limiti d'uso può essere sufficiente una connessione protetta con autenticazione con *user id* e *password* mentre, in assenza di limitazioni, sarà necessario mantenere inalterato il concetto di possesso e conoscenza, prevedendo oltre a *user id* e *password*, l'utilizzo di un sistema O.T.P.[122] (possesso) protetto da P.I.N. (conoscenza)"[123].

Dal punto di vista giuridico, resta pertanto fondamentale garantire la validità della firma digitale sotto la dicotomia del possesso e della conoscenza, indispensabili per il non ripudio del titolare, secondo l'inversione dell'onere della prova previsto dal C.A.D..

Gli H.S.M. consentono di raggiungere notevoli vantaggi sul piano della sicurezza, sia perché permettono di implementare operazioni crittografiche al loro interno (non importano -o esportano- mai le chiavi dall'esterno ma le generano o le distruggono direttamente al loro interno), sia in quanto prevedono delle procedure di autenticazione e autorizzazione al loro utilizzo molto stringenti (autenticazione delle macchine connesse in rete all'H.S.M., *smart card*, PAD numerici e chiavi elettroniche - di plastica - per inizializzazione, riavvio e *back up* dell'apparato)[124]. Inoltre gli H.S.M. si

---

[119] Va tenuto presente che a bordo dell'H.S.M. viene inviato solo ed esclusivamente l'*hash* del documento.

[120] Più precisamente la procedura prevede, prima di effettuare la spedizione dell'*hash*, l'individuazione del certificato da utilizzare e la sua necessaria autenticazione. Al tal fine l'utente si avvale di una *user id* (che tipicamente è il suo codice fiscale) e di una *password* per il suo riconoscimento ed identificazione. Questa *password* serve, a sua volta, per generare un codice di autenticazione temporaneo, restituito al titolare. Costui, quindi, al momento della firma dovrà digitare questo codice (OTP), insieme al PIN (o *password*) e alla *user id*. Solo a questo punto viene inviato l'*hash*, viene attivato il certificato e se tutti i dati inseriti sono corretti, viene creata la firma digitale, che sarà poi rispedita al titolare sul proprio *pc*. Dunque il documento originale si trova in locale, sul *web* viaggia solo l'*hash* e queste autenticazioni, ovviamente attraverso *web services* che si avvalgono di un canale *https*, cioè di una connessione attualmente considerata accettabile sotto il profilo di sicurezza.

[121] I certificati di sottoscrizione, infatti, possono includere limiti d'uso e/o di valore dei negozi per i quali sono attivati. La validità di un certificato, quindi, può essere circoscritta alla sola sottoscrizione degli atti connessi alla carica ricoperta all'interno dell'organizzazione (anch'essa riportata all'interno del certificato) o a quelli che comportano oneri finanziari entro e non oltre un limite monetario predeterminato.

[122] Si tratta di un sistema di *smart card* su cui appare una *One Time Password* (che garantisce il concetto giuridico del "possesso"di un oggetto), protetto da PIN (che garantisce la "conoscenza"di un segreto). L'oggetto del possesso può essere un dispositivo OTP o un telefono cellulare, con la conseguenza che l'OTP potrà essere inviato non solo in locale, ma anche sotto forma di *sms* sul telefono di colui che richiede la firma.

[123] 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.

[124] Scaccia R., *HSM, Hardware Security Module: la grande smart card*, in *http://geekinfosecurity.blogspot.com/2007/12/hsm-hardware-security-module-la-grande.html*

prestano meglio di altri apparati alle operazioni di firma massiva, a cui si ricorre quando il procedimento di sottoscrizione coinvolge un elevato numero di documenti[125]. Attraverso il loro uso, infatti, si evita di dover digitare per ogni documento il P.I.N. di sblocco della *smart card* di firma; l'unica avvertenza che si richiede al titolare è quella di servirsi di una coppia di chiavi diversa da tutte le altre in suo possesso, al fine di poter ricondurre, nel momento della verifica, la firma così generata ad una procedura automatica di sottoscrizione[126]. Infine, gli H.S.M. di nuova generazione, ospitando a bordo migliaia di chiavi crittografiche (cd. multi chiave), consentiranno un abbattimento dei costi per ogni singola firma.

Nonostante la maggior parte degli H.S.M. in commercio non sia certificato secondo lo standard di sicurezza informatica *Common Criteria*[127], questo ostacolo è stato aggirato dal D.P.C.M. del 12/10/2007 pubblicato in G.U. n. 13 del 16/01/2008 allo scopo di sbloccare la situazione di stallo che interessava molti progetti di dematerializzazione documentale. Il decreto in esame ha consentito ai certificatori accreditati di attestare mediante un'autodichiarazione la rispondenza dei vari prodotti e dispositivi di firma, che si avvalgono degli H.S.M., ai requisiti di sicurezza basati su standard riconosciuti, senza dover più attendere l'autorizzazione dall'O.C.S.I.[128]. Questa soluzione non appare tuttavia soddisfacente, lasciando aperto il problema relativo alla conformità degli H.S.M. alla normativa comunitaria.

2.3.3 Generazione dell'impronta e apposizione della firma

La procedura di generazione della firma digitale passa attraverso il calcolo della cd. "impronta" del testo e la sua successiva cifratura con la chiave privata dell'autore. Ciò significa che l'oggetto dell'operazione di cifratura non è il documento in se per sé, ma un suo "riassunto" per così dire, un codice definito tecnicamente "impronta" o *digest*, ottenuto attraverso un algoritmo standard, e quindi ripetibile, da cui prende il nome (funzione di *hash*) [129]. L'*hash* è una stringa di testo di lunghezza prefissata, a prescindere dalla lunghezza del documento originario ed è irreversibile, nel senso che dall'*hash* non si può ricostruire il documento originale; ma si può comunque verificare la sua

[125] Cfr. 2.3.3.

[126] C.N.I.P.A. – Ufficio Sicurezza, *Linee Guida per l'utilizzo della Firma Digitale*, in *http://www.cnipa.gov.it/site/_files/LineeGuidaFD_200405181.pdf*, Maggio 2004.

[127] Tale standard di sicurezza informatica, richiesto dalla Dir. 1999/93/CE e dalla normativa italiana di recepimento per gli usi connessi alla firma digitale, dovrebbe permettere a molte e differenti applicazioni *software* di essere integrate e testate in modo sicuro, vale a dire secondo procedure rigorose e standardizzate.

[128] Ente certificatore italiano sulla sicurezza delle apparecchiature elettroniche, facente capo al Ministero delle Comunicazioni.

[129] Tale scelta è stata compiuta per realizzare la procedura di verifica in breve tempo, evitando di cifrare e decifrare l'intero documento ogni volta; il che obbligava ad inviare un testo in chiaro con allegata una versione dello stesso cifrata con la chiave privata dell'autore e colui che la riceveva, decifrando il testo con la chiave pubblica del mittente, aveva la certezza sull'identità del mittente e sull'integrità del contenuto qualora i due testi fossero risultati identici.

autenticità e la mancanza di alterazioni. Basterà infatti confrontare l'impronta ottenuta dalla decifratura con la chiave pubblica del mittente con quella calcolata attraverso la funzione di *hash* sul testo in chiaro, cioè sul testo originale[130]: se sono uguali significa che il documento proviene da chi appare come il titolare della chiave pubblica e non è stato oggetto di manomissioni successivamente alla generazione della firma.

Dunque, attraverso l'applicazione della chiave privata all'impronta, si avrà la firma digitale, che è appunto l'impronta criptata con la chiave privata dell'autore del documento. La firma così generata può essere associata o separata dal documento, trattandosi di due *file* diversi[131].

Sul punto occorre fare una precisazione: la firma digitale può essere generata secondo due modalità, vale a dire tramite "apposizione" sul documento o "associazione con separata evidenza informatica".

La prima di queste prevede la scrittura del documento in uno spazio preciso individuato dal *software* di firma, in modo che su di esso venga operata una duplice codificazione: sul testo originario si esegue la funzione di *hash* ottenendo l'impronta ed essa, a sua volta, viene codificata mediante l'applicazione della chiave privata[132]. L'insieme di testo e chiave costituisce un'unità indisgiungibile, nel senso che qualunque alterazione del testo impedirà l'uso della chiave pubblica. Il risultato così ottenuto sarà la visualizzazione congiunta del testo e della firma, così come redatto dal mittente[133].

L'associazione della firma a un qualsiasi *file* di memoria prevede, di contro, che il testo venga redatto per mezzo di un comune programma, non pensato unicamente per la creazione della firma, cosicché si avrà la visualizzazione del testo senza l'impronta codificata, la quale si troverà su un diverso *file* di firma. Sarà possibile effettuarne la verifica con le stesse modalità viste in precedenza: la mancata corrispondenza tra chiave pubblica e chiave privata mostrerà che vi è stata una manomissione del testo successiva all'apposizione della firma.

In entrambi i casi la firma digitale sarà visibile sul video, ma nella seconda ipotesi non si tratterà di un unico *file*, ma di un'autonoma indicazione sul video del *file* di firma; il che significa che compariranno due icone, una relativa al testo, l'altra alla firma.

Il titolare può apporre la firma per mezzo di una procedura automatica o manuale di sottoscrizione. La procedura manuale può essere usata limitatamente a un singolo documento.

La procedura automatica, come si è visto, presenta il vantaggio di consentire la sottoscrizione di una pluralità di documenti, senza dover ripetere ogni volta le operazioni necessarie[134]. Sotto il profilo giuridico è però necessario che il firmatario sia a conoscenza di ciò che va a sottoscrivere, seppur non nel dettaglio, perché se ne assume la responsabilità. È sufficiente che questi riceva un'informativa

---

[130] Il che generalmente viene realizzato in automatico dal *software* che, attraverso l'uso della chiave, consente di aprire il documento.

[131] Si potrà avere ad esempio il documento in chiaro accompagnato dalla sua impronta cifrata.

[132] Sia la chiave privata che l'impronta codificata costituiscono delle sequenze alfanumeriche.

[133] Orlandi M., *Firma digitale*, in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*,in *Nuove Leggi civ. comm.*, 2000, III-IV, 751.

[134] In particolare evita di digitare più volte il PIN di sblocco della *smart card*.

sulla tipologia di documenti da sottoscrivere e sulla limitazione d'uso della coppia di chiavi. Il titolare poi, prima di procedere alla sottoscrizione, dovrà accettare esplicitamente tale procedura: deve cioè sussistere la volontarietà di attivare il meccanismo di firma con procedura automatica. Allo stesso modo l'attivazione del dispositivo resta sempre in capo al titolare[135].

La legislazione vigente richiede che il *file* ottenuto dall'operazione rispetti i formati definiti legali in Italia, al fine di garantire l'interoperabilità della firma digitale fra le varie applicazioni[136].

2.3.4 Validazione temporale

La fase conclusiva del processo di firma finora illustrato consiste nell'apporre al documento (o evidenza informatica) un sigillo temporale che ne possa attestare la data e l'ora di esistenza[137]. La validazione temporale riceve definizione per opera del D.P.R. n. 513/97, il quale la identifica all'art. 1 con il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data e un orario opponibili a terzi; definizione confluita interamente nell'art. 1 lett. ab del C.A.D..

Si può notare il differente ruolo svolto dalla data all'interno di una scrittura privata munita di sottoscrizione non autenticata: la data assume una diversa rilevanza probatoria a seconda che sia invocata nei confronti dei terzi o nei rapporti fra le parti. Fra queste ultime, secondo la giurisprudenza costante della Suprema Corte[138], la mancanza o l'incertezza della data può essere colmata ricorrendo ad ogni mezzo di prova previsto dalla legge[139], anche attraverso presunzioni, mentre nei confronti dei terzi essa è opponibile solo dal giorno in cui si sia verificato un fatto da cui possa presumersi, in modo inequivocabile, l'anteriorità della formazione del documento rispetto alla data che le parti vi hanno applicato[140]. Dunque è rimesso al libero apprezzamento del giudice di merito il compito di valutare quale fatto possa considerarsi idoneo a tal fine[141].

---

[135] Manca G., *Ufficio Sicurezza* – C.N.I.P.A.

[136] Con l'entrata in vigore delle nuove regole tecniche la busta crittografica PKCS#7, che è quella più antica, verrà abbandonata e si passerà ad altri formati di busta crittografica, uno dei quali, il CAdES, continuerà a produrre *file* caratterizzati dall'estensione "p7m".

[137] Difatti è possibile firmare un documento oggi (data di formazione) e apporre il sigillo temporale dopo una settimana (data di esistenza).

[138] *Cass. Civ., 13 febbraio 1988, n. 1552*, in *Vita Not.*, 1988, p. 256 e ss; *Rep. Giur. It*., 1988, 3755, p. 11.

[139] Si pensi alla confessione, al giuramento o alla testimonianza.

[140] L'art. 2704 contempla un elenco non tassativo di eventi che costituiscono prova di data certa: *"...dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici (2699) o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento.*" Ciò significa che in mancanza di tali eventi presuntivi le parti non si potranno opporre ai terzi; questo regime più favorevole nei confronti dei terzi si ricollega alla tutela del principio generale dell'affidamento.

[141] Così ad es. l'avviso di ricevimento della racc.ta munita del timbro postale è stato reputato dalla Suprema Corte un mezzo idoneo a conferire certezza alla data della scrittura privata. *Cass. Civ., Sez. I, 12 agosto 1997, n. 7530*, in *Mass. Giust. Civ.*, 1997, p. 1408.

Si può affermare pertanto che "*la validazione temporale del documento informatico assolve la medesima funzione che, per i documenti cartacei, è assolta dai fatti presuntivi che rendono certa e opponibile ai terzi la data della scrittura privata non autenticata*"[142].

Ciò trova conferma altresì nel 3° co. dell'art. 20 del C.A.D., in base al quale la data e l'ora della formazione del documento informatico sono opponibili ai terzi se apposte in conformità delle regole tecniche sulla validazione temporale.

Ne deriva che la datazione risponde all'esigenza di garantire la stabilità probatoria del documento informatico e risolvere le problematiche scaturenti dalla scadenza della firma digitale (*rectius*: del relativo certificato elettronico)[143].

Ciò avviene, materialmente, attraverso l'apposizione al documento informatico della cd. marca temporale, esaminata in dettaglio nel paragrafo seguente[144].

2.3.4.1 La marca temporale

La marca temporale o *time stamping*[145], viene definita dalle nuove regole tecniche approvate con D.P.C.M. 30 marzo 2009 come "*il riferimento temporale che consente la validazione temporale*"[146]. È stato in tal modo sostituito il termine di "evidenza informatica"[147] con quello più specifico e appropriato di "riferimento temporale", mentre si è scelto di non inserire nel nuovo testo la definizione di validazione temporale, restando così valida quella presente nel C.A.D..

La marca temporale è in altre parole una firma digitale di un certificatore che viene apposta ad un documento informatico, già firmato dal suo autore[148] e che deve includere alcune informazioni, tra cui in particolare la data e l'ora di generazione della marca stessa e il valore dell'impronta del documento. Per compiere tale operazione il certificatore si avvale di una coppia di chiavi di certificazione appositamente generata, con la quale sottoscrive il certificato relativo alle chiavi di

---

[142] Buonomo G., *Commento all'art. 1 del D.P.R. 513/97*, in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 653.

[143] Lisi A., Scialdone M., *Il documento informatico e le firme elettroniche*, in *Diritto dell'Internet e delle nuove tecnologie telematiche*, a cura di Cassano G. e Cimino I. P., Cedam ed., 2009, p. 470.

[144] La marca temporale può essere utilizzata altresì per applicazioni diverse dalla semplice apposizione della data su un documento: può essere apposta su un archivio non documentale, come un programma per elaboratore, allo scopo di garantirne la data di pubblicazione (la cd. versione del programma) oppure su un archivio di dati per garantirne l'integrità rispetto a falsificazioni accidentali intervenute dopo la creazione dei documenti o ancora può essere impiegata per l'archiviazione di documenti su supporti alternativi a quello cartaceo.

[145] Un *time-stamp* è una sorta di bollo digitale reso non falsificabile attraverso un sistema di crittografia a chiave pubblica che attesta che il documento è esistito in un particolare momento.

[146] Nel C.A.D. non è presente alcuna definizione né della marca temporale, né del riferimento temporale.

[147] Viene definita come un *file* o una raccolta di dati numerici destinati ad essere trattati unitariamente da un elaboratore elettronico. V. Buonomo G., *Commento all'art. 1 del D.P.R. 513/97* , in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 653.

[148] Al documento, pertanto, verranno associate due firme digitali, quella del sottoscrittore e quella del soggetto che ha effettuato la validazione temporale. Anche le nuove regole tecniche, analogamente alle previgenti, prevedono che le marche temporali siano firmate digitalmente (art. 43, co. 2°, lett. c).

marcatura temporale[149]. Il procedimento seguito non si distingue, sotto il profilo tecnologico, dalla sottoscrizione digitale del documento. L'intervento di tale soggetto terzo è "*in grado di rendere anche la data, così come la sottoscrizione, valida e rilevante a tutti gli effetti ed opponibile ai terzi*"[150].

Con ciò si vuole intendere che la marca viene utilizzata per avere un riferimento temporale opponibile a terzi dell'esistenza di un documento sottoscritto. Infatti, chi intende avvalersi della firma, potrebbe avere l'esigenza, dal punto di vista giuridico, di dover provare la sua validità ed esistenza in un determinato momento. Costui, dunque, potrà dimostrare, qualora il titolare revochi il suo certificato[151] o questo sia scaduto in un momento successivo, che la firma è stata apposta antecedentemente alla revoca o alla scadenza e quindi continua ad essere valida.

Al riguardo l'art. 37 del decreto in esame, rubricato "riferimenti temporali opponibili a terzi", ribadisce che costituiscono validazione temporale: il riferimento temporale contenuto nella segnatura di protocollo delle amministrazioni pubbliche; il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione[152]; il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del C.A.D.. Ad esse viene aggiunto nel nuovo testo il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica[153], assieme alla previsione che i suddetti riferimenti temporali possono essere utilizzati da chiunque e non solo dalle P.A.[154]. Ciò significa che, anche nei rapporti fra privati, essi avranno un'efficacia probatoria e potranno essere utilizzati per far valere gli atti sui quali sono apposti nei confronti di terzi.

L'art. 50 del D.P.C.M. in esame conferma la precedente disciplina secondo cui l'evidenza informatica alla quale si applica la marca può essere costituita sia dall'intero documento, sia dal valore della sua impronta o di più impronte[155]. Al riguardo si precisa in dottrina che la marca non fornisce indicazioni sul momento in cui il documento è stato formato o inviato, ma si limita ad attestare il

---

[149] Occorre, infatti, tenere distinte le chiavi destinate alla sottoscrizione elettronica da quelle destinate alla marcatura temporale che, pur essendo tecnicamente uguali, hanno uno scopo e un significato giuridico differente.

[150] Sarzana Di Sant'Ippolito F., C*onsiderazioni in tema di documento informatico, firma digitale e regole tecniche*, in *Corriere Giuridico*, 1999, 7, p. 802.

[151] Ad es. in caso di smarrimento della *smart card*.

[152] Va ricordato che sul tema è intervenuta di recente la L. n. 2/2009 la quale ha modificato i co. 4° e 5° dell'art. 23 del C.A.D., eliminando la figura del pubblico ufficiale tenuto all'apposizione della marca temporale. In particolare al co. 5° si prevede che costui debba limitarsi, nel processo di conservazione ottica sostitutiva, a firmare digitalmente la dichiarazione con la quale attesta la conformità della copia su supporto informatico all'originale del documento analogico unico, giudicato tale in base ad individuazione operata con D.P.C.M.. Il 4° co., invece, non contempla più la categoria dei documenti analogici originali non unici e la figura del responsabile della conservazione, disponendo che "*Le copie su supporto informatico di qualsiasi tipologia di documenti analogici originali, formati in origine su supporto cartaceo o su altro supporto non informatico, sostituiscono ad ogni effetto di legge gli originali da cui sono tratte se la loro conformità all'originale è assicurata da chi lo detiene mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche [..]*".

[153] A seguito della pubblicazione del D.M. 21 gennaio 2008.

[154] È stato, infatti, eliminato dall'art. 37 (già art. 39 nel D.P.C.M. 13 gennaio 2004) l'inciso che riconosceva alle P.A. la possibilità di utilizzare come sistemi di validazione temporale anche quelli pocanzi menzionati.

[155] Che sono il risultato del calcolo mediante funzione di *hash*.

momento in cui è stata generata[156]. Questa fase, infatti, avviene di solito in via telematica per mezzo di un apposito *software*, tramite il quale si effettua la richiesta di validazione temporale e la si inoltra al servizio di marcatura temporale presso il certificatore. Sarà poi questo servizio a procedere in automatico alle operazioni di apposizione della marca, sottoscrizione con firma digitale e restituzione del relativo *file* all'utente[157]. Tale procedura consente, a chiunque sia in possesso del documento e della marca temporale, di verificare nei registri dei certificatori la presenza di eventuali revoche o sospensioni, che possono compromettere l'efficacia della validazione temporale[158].

In relazione alla validità delle marche temporali, va ricordato che nel previgente quadro normativo, sulla base dell'art. 50 del D.P.C.M. 13 gennaio 2004, i termini di conservazione non potevano essere inferiori ai cinque anni e la validità delle marche veniva subordinata al periodo di conservazione a cura del fornitore del servizio, con la conseguenza che trascorsi i cinque anni, i documenti marcati temporalmente rischiavano di non avere più la stessa rilevanza civilistica/fiscale[159]. Ne derivava quindi anche l'impossibilità di opporre a terzi la data ottenuta con la procedura di validazione temporale, che esauriva i suoi effetti alla scadenza del certificato utilizzato per generarla, salvo apposizione di una nuova marca temporale prima della suddetta scadenza; in modo simile al compimento di un atto interruttivo della prescrizione.

Per superare tale rischio, che contribuiva a creare un clima di sfiducia nei confronti della firma digitale, sono state introdotte, dal D.P.C.M. 30 marzo 2009, alcune modifiche che mirano ad allungare la vita della marca temporale e di riflesso della firma digitale.

La prima di queste importanti novità è contenuta nell'art. 49 del D.P.C.M. in commento, in base al quale tutte le marche temporali generate saranno conservate in un apposito archivio digitale non modificabile per almeno vent'anni o, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore[160]. Ciò significa che anche la loro validità sarà estesa per almeno vent'anni, in modo da coordinarsi con il dettato del C.A.D. che dispone la conservazione degli elementi utili in sede processuale per il medesimo periodo. In altre parole, qualora il certificatore venga chiamato in giudizio in merito alla validità di una marca temporale, potrà dichiarare che la stessa, pur essendo basata su algoritmi non più sicuri in quel momento, è stata da lui generata

[156] Lisi A., Scialdone M., *Il documento informatico e le firme elettroniche*, in *Diritto dell'Internet e delle nuove tecnologie telematiche*, a cura di Cassano G. e Cimino I. P., Cedam ed., 2009, p.471.

[157] Il *file* marcato temporalmente ha estensione "m7m" e racchiude il documento del quale si è chiesta la validazione temporale e la marca emessa da parte del soggetto terzo "certificatore".

[158] Tale verifica si effettua attraverso l'uso della chiave pubblica abbinata alla chiave privata impiegata dal certificatore per apporre la marca temporale.

[159] Silipigni G., *La nuova marca temporale allunga la vita alla firma digitale*, 08/06/2009, in *http://www.nuovofiscooggi.it/attualita/articolo/la-nuova-marca-temporale-allunga-la-vita-alla-firma-digitale*.

[160] L'art. 49 co. 2° dispone la loro validità per il periodo di conservazione stabilito o concordato con il certificatore. Rispetto al precedente regolamento, si introduce la possibilità di concordare il periodo di conservazione con il certificatore, lasciando dunque discreti margini di flessibilità.

vent'anni prima, quando gli algoritmi erano sicuri e quindi mantiene la sua validità[161]. Si è voluto, in tal modo, salvaguardare la validità delle marche temporali, evitando di dover rimarcare periodicamente tutti i documenti[162].

La nuova disciplina potrebbe così condurre l'interprete alla conclusione apparentemente logica, ma non esauriente, che la conservazione della marca temporale sia sufficiente per garantirne la validità, a prescindere dall'effettiva possibilità di verificare la firma digitale utilizzata per la marcatura. In proposito la dottrina si era già pronunciata in passato, giudicando il disposto dell'art. 50 co. 2° delle abrogate regole tecniche del 2004, che statuiva parimenti la validità della marca per il periodo di conservazione, come un ulteriore requisito per la validità delle marche temporali, al fine di aumentare la sicurezza delle regole tecniche, ma certamente di per sé non bastevole, richiedendosi sempre la procedura di verifica[163].

Infine, vanno menzionati i vantaggi, dal punto di vista pratico, che la nuova formulazione dell'art. 43 consentirà di realizzare. In particolare il co. 3° del suddetto articolo introduce *ex novo* la possibilità di apporre una marca temporale ad un documento informatico che contiene un insieme di impronte. Ciò significa che in presenza di una pluralità di documenti non sarà più necessario apporre su ciascuno di essi una marca, e dunque sostenerne i relativi costi, ma si potrà formare un solo documento contenente le impronte di tutti i documenti, al quale applicare una sola marca temporale, cioè un riferimento temporale opponibile a terzi. Si è riscontrato[164] che la novità rispetto al passato sta nella possibilità di scindere uno o più documenti dall'intero lotto senza perdere l'efficacia della marca stessa; il che era finora impraticabile data la presenza di un'unica impronta per un lotto di più documenti, alla quale veniva apposto il riferimento temporale[165].

Sempre in materia fiscale, occorre menzionare il nuovo art. 2215 bis c.c. che prevede l'apposizione della marcatura temporale e della firma digitale ogni tre mesi per assolvere agli obblighi inerenti la regolare tenuta informatica di libri, repertori e scritture[166]. Si ritiene[167] al riguardo che

---

[161] Infatti la firma digitale del certificatore, con la quale viene apposta la marca temporale, è basata sugli stessi algoritmi crittografici che caratterizzano la firma digitale utilizzata per sottoscrivere un documento, i quali sono soggetti ad un'inevitabile obsolescenza sotto il profilo tecnico e quindi della sicurezza.

[162] Evitando cioè di emettere nuove marche temporali ogni "n" anni. Ciò sarebbe devastante non tanto per il costo della singola marca, quanto per i costi gestionali complessivi. Si pensi ad una P.A. o un'azienda costretta a rimarcare periodicamente migliaia di documenti.

[163] Pelosi A., *Le nuove regole tecniche relative ai documenti informatici di cui al D.P.C.M. 13 gennaio 2004*, in *Contratti*, 2004, 8/9, p. 836.

[164] Giordano F., *Firma digitale: nuove regole per agevolare gli operatori*, in *http://icpressroom.wordpress.com/2009/07/02/firma-digitale-nuove-regole-per-agevolare-gli-operatori/*.

[165] La nuova modalità consente, nell'esempio del commercialista, di creare un impronta per ciascun cliente dello Studio, di raccogliere tutte le impronte in un unico documento e di apporvi una sola marca temporale. In questo modo sarà possibile per il commercialista consegnare a ciascun cliente dello Studio esclusivamente i propri registri (e non anche quelli di tutti i clienti dello Studio) accompagnati dal documento contente tutte le impronte (compresa quella del cliente in essere) e dalla marca temporale apposta sul suddetto *file*.

[166] Attività che esula dall'annuale processo di conservazione digitale dei libri obbligatori e delle altre scritture contabili, il quale richiede l'apposizione sull'insieme dei documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti informatici, della firma digitale e della marca temporale a cura del responsabile della conservazione.

l'imprenditore dovrà garantire la datazione, l'autenticità e l'integrità, attraverso la precedente apposizione di una marcatura temporale interna, intesa come "riferimento temporale", cosicché i dati integri ed inalterabili, saranno sempre consultabili e attesteranno la sequenzialità cronologica delle operazioni eseguite. Va precisato che questa operazione serve solo a garantire una corretta formazione del documento[168] contenente le registrazioni relative ai tre mesi precedenti, in modo che esso possa "civilisticamente" assolvere le funzioni di numerazione progressiva e vidimazione. La natura di tali documenti, soggetti per definizione ad aggiornamento continuo, richiede, infatti, la loro "cristallizzazione" nel tempo, per poter assumere il valore giuridico di documento informatico.

2.3.4.2 Valore della firma digitale nel tempo

La firma digitale, pur offrendo maggiori garanzie sotto il profilo dell'integrità e della paternità di un documento, presenta un punto debole rispetto alla sottoscrizione cartacea: mentre quest'ultima resta valida indipendentemente dal trascorrere del tempo[169], la validità della firma digitale è legata a quella del certificato elettronico ad essa relativo (solitamente triennale).

Questa disparità di trattamento comporta che una firma digitale o un altro tipo di firma elettronica qualificata apposta dopo la scadenza, revoca o sospensione del relativo certificato perde automaticamente la sua efficacia probatoria, per ridursi a mancata sottoscrizione (art. 21, 3° co. C.A.D.). In particolare la revoca o la sospensione del certificato ne producono rispettivamente l'annullamento o la sospensione della validità[170].

Si era posto, altresì, il problema se i documenti sottoscritti digitalmente prima della scadenza, revoca o sospensione potessero considerarsi ancora validi. La dottrina maggioritaria[171] ha ritenuto che tali eventi non siano dotati di efficacia retroattiva ma che producano effetti solo per il futuro, vale a dire dal momento della pubblicazione[172]; in secondo luogo ha identificato tale validità non nell'assenza di difetti formali o strutturali, cioè nell'immunità del certificato da vizi, ma nella

---

[167] Lisi A., Zingarelli S., *Commento al nuovo art. 2215 bis cod. civ.: 'marcatura temporale' e 'marca temporale'*, in *http://www.diritto.net/content/view/3750/6/*.

[168] Attraverso la garanzia di immodificabilità e staticità fornita dalla firma digitale.

[169] Non esiste, infatti, alcuna norma che statuisca il valore di una firma autografa nel tempo, semmai è il documento che può avere la validità espressa nei contenuti. Con ciò si intende che se due soggetti redigono un contratto, esprimendo chiaramente la loro volontà ed apponendo insieme la data, essa resta valida, salvo che uno dei due la disconosca.

[170] Come si ricavava dall'art. 52 del D.P.C.M. 13 gennaio 2004.

[171] Vedi tra tutti Spaziani P., in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 738; Orlandi M., in Bianca (a cura di), Ibidem, in *Nuove Leggi civ. comm.*, 2000, III-IV, 757 e ss; Graziosi A., *La nuova efficacia probatoria del documento informatico*, in *Rivista trim. di dir. proc. civ.* , 2003, 01, p. 62 e ss.

[172] Con conseguente impossibilità di imputare al titolare le scritture firmate successivamente, ma senza travolgere quelle precedenti, che mantenevano la loro validità.

possibilità di opporre al titolare della chiave pubblica i dati in esso contenuti[173]. Ciò comportava, viceversa, che a seguito della revoca o della sospensione i terzi non potevano più opporre al titolare della chiave pubblica le informazioni contenute nel certificato. Dall'analisi di tale orientamento appare evidente come la validità attenga alla capacità probatoria del documento, il quale a seguito della scadenza o della revoca si indebolirebbe, cioè sarebbe di per sé incapace di provare la paternità del testo, impedendone l'imputazione [174].

Per superare queste criticità e protrarre nel tempo la validità dei documenti era necessario apporre sugli stessi una marca temporale prima della scadenza del certificato qualificato, secondo il disposto dell'art. 52 del D.P.C.M. 13 gennaio 2004[175], in base al quale "*la validità di un documento informatico, i cui effetti si protraggono nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una marca temporale*".

A semplificare tale procedura ha contribuito l'art. 51 delle nuove regole tecniche, in forza del quale la firma digitale resta valida nel tempo, anche dopo la scadenza, la sospensione o la revoca del relativo certificato qualificato, purché sia associabile alla stessa un riferimento temporale opponibile a terzi, che renda la generazione della firma collocabile con certezza in un momento precedente alla sopravvenuta invalidità del certificato[176].

Di conseguenza, con l'entrata in vigore delle citate regole tecniche, è auspicabile che il legislatore tenga conto della possibilità di avvalersi dei riferimenti temporali pocanzi menzionati al fine di attribuire qualche valore anche a quelle firme apposte dopo la scadenza del certificato, qualora ne sussistano i presupposti, in modo da attenuare la rigidità dell'art. 21, 3° co. C.A.D. che le equipara a mancata sottoscrizione.

Con la novellazione ora esaminata, se da un lato si è ridotto il rischio della perdita di efficacia probatoria del documento informatico, dall'altro si continua ad affermare in termini giuridici che la firma non è valida se non è fornita di data certa, determinata o determinabile. Dunque, permane la distinzione rispetto ad una sottoscrizione autografa, che resta valida anche se priva di data certa, e quantomeno non necessita della prova di esistenza in vita alla data in cui la medesima è stata

[173] Questa interpretazione dottrinale si basava sul disposto dell'art. 1, lett. p del D.P.R. 513/97, poi trasfuso nell'art. 22, lett. n del D.P.R.445/00, così come modificato dall'art.8 del D.P.R.137/03, ove all'espressione "validità del certificato" veniva riconosciuto il medesimo significato. Sarà compito della dottrina trovare un nuovo fondamento alla suddetta interpretazione, vista l'assenza nel C.A.D. della definizione di "validità del certificato". Infatti, l'art. 28 lett. f del Codice si limita a richiedere che i certificati qualificati contengano alcune informazioni, tra cui l'indicazione del termine iniziale e finale del periodo di validità del certificato, senza fornire ulteriori chiarimenti.

[174] Orlandi M., in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 757 e ss.

[175] Già art. 60 del D.P.C.M. 8 febbraio 1999, che prevedeva l'apposizione di una o più marche temporali.

[176] Ciò significa che per garantire la validità di un documento nel tempo, sarà possibile, oltre ad apporvi successivamente alla firma digitale una marca temporale, anche ricorrere alle altre ipotesi di riferimento temporale (seppure queste non offrono le medesime garanzie della marca, intesa quale firma digitale del "terzo certificatore"). Vedi sul punto par. 2.3.4.1 pp. 31-32.

apposta[177]. L'indicazione della data non costituisce elemento essenziale della scrittura privata, sebbene non possa prescindersi dalla determinazione temporale della documentazione privata attraverso cui si realizza[178].

La diversa disciplina che contraddistingue la firma digitale trova giustificazione nell'esigenza di garantire, ai fini di sicurezza, di poter risalire ad una data certa, data l'eventualità che il certificato sia scaduto, revocato o sospeso. "*Il riconoscimento della validità giuridica della data del documento informatico e della sua opponibilità ai terzi consente di isolare il requisito della data conferendo ad essa valore giuridico autonomo, in ogni caso, dal documento a cui è apposta*"[179]. La data si viene così a configurare, per mezzo dell'applicazione di un riferimento temporale, come un elemento ultroneo, separato dalla firma.

Questa soluzione è stata criticata da quanti ritenevano più idoneo approntare un meccanismo di firma che consentisse di inserire nel documento sottoscritto anche l'indicazione della data e dell'ora di utilizzazione della chiave di sottoscrizione, includendo la chiave di marcatura temporale all'interno del dispositivo di firma[180]. Il che avrebbe consentito di far diventare la data parte integrante del documento, analogamente a quanto si verifica per la scrittura privata cartacea, ma avrebbe impedito di rendere opponibile con certezza la data a terzi.

L'unico modo che, ad oggi, continua ad applicarsi per attribuire certezza all'identità del sottoscrittore ed alla data da esso apposta è l'autonoma previsione di una chiave di validità temporale differente dalla semplice chiave di sottoscrizione e la necessaria presenza dell'Autorità di Certificazione nell'apporre il sigillo temporale con un procedimento esterno all'*iter* di formazione della chiave di sottoscrizione[181].

Sarebbe forse più opportuno che il nuovo art. 51, piuttosto che lasciar intendere la totale invalidità di una firma sprovvista di data, chiarisca semplicemente che in una simile ipotesi la firma non potrà essere temporalmente collocabile, con impossibilità di associare alla stessa tutta una serie di conseguenze legate al trascorrere del tempo[182].

D'altra parte, se l'intento del C.A.D. è quello di compiere l'equiparazione fra firma autografa e digitale, come previsto nell'art. 21 co. 2°, non dovrebbero porsi ancora questi problemi: tali firme dovrebbero essere uguali a tutti gli effetti giuridici. Se invece restano dubbi sulla loro equivalenza, a

---

[177] La mancanza di autonomia funzionale della data rispetto al documento cartaceo consente alle parti di dichiarare in Tribunale di aver apposto la sottoscrizione autografa in un determinato giorno. Anche qualora vi fossero dubbi, generati dall'uso di un inchiostro che scompare con il tempo, quella firma resta valida se le parti o un terzo non la contestano. Nel caso della firma digitale, di cui sia scaduto, revocato o sospeso il certificato, sembrerebbe , invece, che la firma sia invalida se priva di data certa, a prescindere dalla presenza di un terzo che vi si opponga.

[178] Giacobbe, voce Data, in Enc. Dir., vol. XI, p.694.

[179] Sarzana Di Sant'Ippolito F., C*onsiderazioni in tema di documento informatico, firma digitale e regole tecniche*, in *Corriere Giuridico*, 1999, 7, p. 802.

[180] In modo tale da ridurre il numero delle chiavi ed evitare un appesantimento delle procedure di validazione della firma digitale; parere espresso dall'ALCEI (Associazione per la libertà nella comunicazione elettronica interattiva) in *http://www.alcei.it/index.php/archives/6.*

[181] Sarzana Di Sant'Ippolito F., Ibidem, in *Corriere Giuridico*, 1999, 7, p. 802.

[182] Si pensi ai diritti, interessi legittimi, prescrizioni, interessi ecc.

prescindere dal profilo tecnico in cui appare evidente la diversità, ma limitandosi a considerare l'aspetto giuridico della loro validità, allora ci si dovrà scontrare con la resistenza del mondo ad accettare la firma digitale ed a sostituirla alla sottoscrizione autografa.

2.3.5 Verifica della firma digitale

La verifica della firma digitale non corrisponde al cd. processo di verificazione previsto per la sottoscrizione autografa dagli artt. 216 e ss. del c.p.c., in base al quale una parte chiede di accertare l'autenticità della scrittura o della sottoscrizione di una scrittura privata, a seguito del suo disconoscimento per opera della controparte, indicando le scritture che possono servire di comparazione[183]. Questa operazione non può essere compiuta quando l'oggetto sia un documento informatico che per sua natura, essendo privo di un legame "fisico" con il suo autore, non si presta ad essere confrontato con altri documenti informatici. La verifica della sua provenienza può essere compiuta solo attraverso il riscontro della corrispondenza della doppia chiave asimmetrica a quel determinato soggetto, nonché dei dati riportati dal certificato, asseverata da un certificatore nei registri a ciò dedicati; salvo poi che il presunto sottoscrittore riesca a provare l'utilizzo abusivo del dispositivo di firma, a seguito della sua sottrazione indebita o della falsità della certificazione[184].

Il legislatore, pertanto, allo scopo di predisporre una disciplina che si adattasse alle peculiari caratteristiche del documento informatico, ha modificato più volte le disposizioni inerenti all'efficacia probatoria. Nel paragrafo successivo si illustreranno le modifiche intervenute e ci si soffermerà in particolare sulla disciplina della firma digitale, non essendo possibile in questa sede esaminare nel dettaglio tutte le altre ipotesi, poiché ciò porterebbe oltre la finalità del nostro intento.

2.3.5.1 Il valore probatorio e l'efficacia giuridica delle sottoscrizioni informatiche

Se inizialmente il D.P.R. n.513/97 e il T.U. n.445/2000[185] attribuivano al documento informatico sottoscritto con firma digitale (o altro tipo di firma elettronica qualificata) l'efficacia di scrittura privata ex art. 2702 c.c.[186]; a seguito del recepimento della direttiva 1999/93 CE, si decise di attribuire ad esso una forza probatoria più elevata, simile a quella della scrittura privata autenticata di

[183] Il giudizio di verificazione può essere richiesto davanti al giudice anche dal presunto autore che disconosca la firma autografa a lui attribuita nel caso di abusi o falsificazioni. Solo nel caso di vittorioso esperimento della procedura di verificazione, la scrittura disconosciuta può acquistare valore di prova, essendo preclusa al giudice ogni diversa valutazione.

[184] Cfr. par. 2.2.2.

[185] Art. 10 co. 3°.

[186] Vale a dire qualunque documento scritto e sottoscritto dalle parti con firma autografa, che fa piena prova della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta, salvo che la scrittura sia impugnata con querela di falso.

cui all'art. 2703 c.c.[187], e cioè la piena prova fino a querela di falso[188]. In tal modo se il titolare della chiave privata disconosceva la propria firma doveva proporre querela di falso e fornire le necessarie prove, a differenza della situazione preesistente in cui la prova doveva essere esibita da colui che chiedeva il riconoscimento della scrittura disconosciuta dal suo presunto autore[189].

Si è rilevato in dottrina come tale regime probatorio "*meglio abbia tutelato lo sviluppo della giovane e purtroppo debole e minacciata vita della firma digitale*"[190]. Si argomenta al riguardo che, non esistendo nel nostro ordinamento una normativa specifica sul disconoscimento e sulla verificazione di un documento informatico sottoscritto digitalmente, l'estensione della semplice efficacia di scrittura privata porterebbe alla conseguenza di rendere estremamente agevole disconoscere un siffatto documento, così da degradarlo ad una riproduzione meccanica[191].

La diversa scelta compiuta ha voluto dunque scongiurare il rischio di giungere per tale via alla scomparsa della firma digitale. Se, infatti, si applicasse il principio generale del processo civile che pone l'onere della prova a carico dell'attore (art. 99 c.p.c.), si costringerebbe chi ha prodotto in giudizio il documento sottoscritto digitalmente, in caso di un suo disconoscimento, a dare dimostrazione della provenienza non solo con riferimento alla validità della chiave pubblica al momento della sottoscrizione, ma altresì relativamente all'uso del dispositivo di firma da parte del titolare medesimo[192]. Il che si tradurrebbe in una prova diabolica, qualora la sottoscrizione digitale non sia avvenuta alla presenza di un terzo, e vanificherebbe tutti gli sforzi atti a rendere affidabile la firma digitale, perché a fronte dell'impossibilità di dimostrarne la veridicità nessuno vorrebbe più farne uso.

Nel contempo, però, si deve riconoscere che anche l'efficacia fino a querela di falso non è esente da effetti negativi. L'inversione dell'onere della prova a carico del titolare della firma digitale obbligherebbe costui, per liberarsi degli effetti di una firma digitale apposta illecitamente da altri, ad interrompere il processo civile ed a promuovere, tramite querela di falso, un apposito procedimento davanti al Tribunale in composizione collegiale, con l'intervento del P.M.[193].

---

[187] Senza però attribuirgli tale classificazione, vista la mancanza di un soggetto preposto ad attribuire la fede pubblica.

[188] Pertanto l'efficacia di "piena prova" non dipendeva più dal riconoscimento, sia pure tacito, per mancato disconoscimento, della persona nei cui confronti il documento informatico veniva fatto valere, ma era *in re ipsa*.

[189] Lisi A., Scialdone M., *Il documento informatico e le firme elettroniche*, in *Diritto dell'Internet e delle nuove tecnologie telematiche*, a cura di Cassano G. e Cimino I. P., Cedam ed., 2009, p. 462.

[190] Neirotti L, *Riflessioni giuridiche sulla firma elettronica:limiti, problemi, prospettive*, in *Cyberspazio e diritto*, 2005, vol. 6, n.3, p. 401.

[191] Il sottoscrittore, infatti, semplicemente disconoscendo la propria sottoscrizione, cioè negando che quella che appare essere la sua firma sia stata apposta da lui, può far crollare l'efficacia probatoria della scrittura privata.

[192] Occorrerebbe cioè provare che è stato effettivamente il titolare ad utilizzare materialmente il dispositivo sicuro di firma al fine di effettuare la sottoscrizione elettronica.

[193] Il procedimento si svolge comunque in sede civile, ma è necessaria la presenza del P.M. perchè in caso sia verificato il falso (*rectius*: l'abuso da parte di terzi) si passa automaticamente in sede penale.

Per i motivi ora esaminati si è cercato di trovare una soluzione di compromesso in grado di bilanciare gli interessi delle parti, da un lato non consentendo al titolare un disconoscimento di comodo e dall'altro sollevando la controparte dall'onere di una prova quasi impossibile[194].

A tal fine è stata introdotta nell'art. 21, co. 2° del C.A.D.[195]una presunzione *iuris tantum* di attribuibilità dell'utilizzo del dispositivo sicuro in capo al titolare, salvo che questi provi il contrario. Il titolare, dunque, può dichiarare già durante il processo ordinario di cognizione l'utilizzo abusivo del dispositivo di firma e liberarsi degli effetti connessi dando prova, con qualsiasi mezzo, che l'utilizzo non è a lui riconducibile[196], senza neppure dover proporre querela di falso.

Si è dunque ritornati all'efficacia probatoria della scrittura privata, con i correttivi esaminati, e all'efficacia fino a querela di falso solo nell'ipotesi di riconoscimento da parte del titolare o mancato disconoscimento[197].

Per quanto riguarda il documento con la firma elettronica cd. semplice nell'art. 21, co. 1° del C.A.D. viene stabilito che la sua efficacia probatoria sia rimessa alla libera valutazione del giudice, in considerazione delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità. Ciò significa che se il documento munito di firma elettronica semplice non viene disconosciuto manterrà il valore di piena prova; in caso contrario gli verrà attribuita dal giudice un'efficacia commisurata al grado di certezza che la firma può garantire nella singola situazione. Con questa disposizione il legislatore ha dunque chiarito che solo la firma digitale o altro tipo di firma elettronica qualificata conferisce il valore di prova legale, mentre la firma elettronica debole non conferisce alcuna efficacia probatoria privilegiata.

Se ci si sposta sul piano sostanziale si può ravvisare, parimenti, una differente disciplina tra le due tipologie di firma nell'art. 20 del C.A.D., laddove si precisa al co. 1° bis che "*l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità*" [198], e al 2° co. che il documento informatico sottoscritto con firma digitale soddisfa

---

[194] Neirotti L, *Riflessioni giuridiche sulla firma elettronica:limiti, problemi, prospettive*, in *Cyberspazio e diritto*, 2005, vol. 6, n.3, p. 404 e ss.

[195] "*2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria*".

[196] Non è sufficiente, dunque, un mero disconoscimento formale, ma egli dovrà allegare prova del mancato utilizzo o dello smarrimento o del furto dello strumento di firma.

[197] È per questa ragione che il Consiglio di Stato, nel parere espresso sullo schema del D. Lgs. correttivo del C.A.D., ha configurato il documento informatico dotato di firma digitale come un "*tertium genus tra la scrittura privata e l'atto pubblico, avendo in giudizio la stessa efficacia probatoria di una scrittura privata munita di una sottoscrizione legalmente riconosciuta, ed essendo in realtà, in nulla diverso da una scrittura privata munita di sottoscrizione non autenticata*"; *CdS , Parere 30 gennaio 2006, n. 31.*

[198] Questo comma è stato introdotto dal D. Lgs n. 159/06, a seguito delle critiche mosse dal Consiglio di Stato e dalla dottrina circa la scelta iniziale del legislatore del Codice di non specificare l'efficacia formale del documento informatico sottoscritto con firma elettronica semplice, come a reputarlo insufficiente ad integrare il requisito della forma scritta. Si osservava al riguardo che la natura scritta di un documento non è legata al requisito soggettivo della sottoscrizione, ma a quello oggettivo dell'integrità ed inalterabilità, cioè alla sua attitudine a cristallizzare una certa rappresentazione nel tempo. Vedi sul tema Minerva M., *Documento informatico e forma scritta*, in

comunque il requisito della forma scritta. Nel 2° co., in effetti, si riconosce esplicitamente, in presenza di firma digitale, la sussistenza del requisito legale della forma scritta: si tratterebbe, dunque, di quei casi in cui la forma, prescritta *ad substantiam*, è quella della scrittura privata[199]. Nel co. 1° bis, invece, si farebbe riferimento al documento scritto con firma elettronica semplice o privo di sottoscrizione (cd. mera forma scritta), il cui valore formale è rimesso alla libera valutazione del giudice[200]. Si ricava dunque, dalla lettura congiunta dell'art. 20 co. 1° bis e dell'art. 21, co. 1°, che il giudice è chiamato a svolgere una duplice valutazione: la prima sul piano formale, la seconda su quello probatorio.

Infine, per quanto concerne il documento informatico privo di firma, già il T.U.D.A. estendeva ad esso l'efficacia probatoria prevista per le riproduzioni meccaniche di cui all'art. 2712 c.c., ed ora il C.A.D. ha provveduto ad integrare la disciplina del codice civile inserendo nella norma citata la categoria delle riproduzioni informatiche[201], così come disposto dal 1° co. dell'art. 23, confermando che esse formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime[202].

Giurisprudenza[203] e dottrina[204] hanno osservato che il disconoscimento, pur privando la riproduzione meccanica dell'efficacia di prova legale, avendo ad oggetto fatti e non regole, non preclude al giudice la possibilità di utilizzare liberamente il documento, qualora lo reputi attendibile, per formare il proprio convincimento[205]. Ovviamente sarà onere di colui che intenda far valere le riproduzioni, provare con ogni mezzo la loro conformità ai fatti e alle cose che esse rappresentano, o

---

www.interlex.it/forum10/relazioni/30minerva.htm; Parere del Consiglio di Stato n. 11995, Adunanza del 7 febbraio 2005, in *Giur. It.*, 2005, I, p. 1163.

[199] In tal modo la scrittura privata elettronica viene equiparata a quella tradizionale, in base al giudizio *ex ante* del legislatore che reputa la firma digitale o qualificata necessaria e sufficiente a tal fine e non lascia spazio ad alcuna valutazione del giudice.

[200] Così ad es. i documenti informatici soddisfano il requisito della forma scritta se conformi ad alcuni standard tecnici, tra cui in particolare l'XML, che consente la classificazione e l'inserimento dei dati secondo un *format* comune strutturato in campi predefiniti, in modo da garantire l'uniformità a livello informatico.

[201] Ne deriva che può costituire rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti un *file* audio o video, come la diffusione di suoni, la trasmissione di immagini memorizzata in un *cd rom*, la visualizzazione di immagini fotografiche, ecc. Si può quindi ravvisare la forma scritta in presenza di qualsiasi rappresentazione grafica impressa su supporto durevole, anche privo di sottoscrizione.

[202] In tal senso si è espressa anche la giurisprudenza con sent. *Cass. Civ. 6/12/01, n. 11445,* in *Rep. Foro It.*, 2001.

[203] "*Il disconoscimento della conformità di una copia fotostatica all'originale di una scrittura non ha gli stessi effetti del disconoscimento previsto dall'art. 215, 2° co. c.p.c., perché mentre quest'ultimo, in mancanza di richiesta di verificazione e di esito positivo di questa, preclude l'utilizzazione della scrittura, il primo non impedisce che il giudice possa accertare la conformità all'originale anche attraverso altri mezzi di prova, comprese le presunzioni*"; *Cass. Civ., 4/3/2004, n. 4395* , in *Rep. Foro It.*, 2004.

[204] "*mentre nel caso della scrittura privata disconosciuta - se non si effettua un'ulteriore attività di verifica – non sopravvivono elementi in grado di contribuire alla formazione del convincimento del giudice, mancando ogni possibilità di confronto oggettivo tra ciò che risulta dal documento e la verità dei fatti rappresentati, nel caso delle riproduzioni meccaniche - grazie soprattutto alla più recente evoluzione tecnica – è spesso possibile un accertamento oggettivo e immediato della conformità dei fatti rappresentati a quelli accaduti. Analoghe considerazioni devono valere a maggior ragione per il documento informatico che presenti sufficienti requisiti per garantirne l'identificazione del suo autore e la mancanza di alterazioni*".Patti S., *L'efficacia probatoria dei "nuovi" documenti informatici*, in *http: /www.tribunaletrieste.it/documenti/relazioni/salvatore_patti.htm*, 2003, p. 4.

[205] Il documento, dunque, pur non costituendo una prova legale, può essere considerato una prova semplice, come tale liberamente valutabile dal giudice ai sensi del co. 1° dell'art. 116 c.p.c.: "il giudice deve valutare le prove secondo il suo prudente apprezzamento, salvo che la legge disponga altrimenti". Ne consegue che il documento informatico privo di firma digitale resta liberamente valutabile sul piano probatorio, tanto se non sottoscritto quanto se sottoscritto con firma elettronica debole.

viceversa la loro inidoneità a fornire una corretta rappresentazione della realtà e dei dati. Diversamente, in mancanza di disconoscimento[206], dunque di fatto non contestato, l'efficacia del mezzo di prova è sottratta alla libera valutazione del giudice e si può parlare di prova legale.

Orbene, da quanto esposto si ricava una differente scelta dell'ordinamento, quella cioè di attribuire maggiore affidabilità al documento informatico privo di firma rispetto al documento cartaceo non sottoscritto, per il quale non è invocabile, di per sé solo, alcuna efficacia probatoria.

A parere di chi scrive la parziale modifica dell'art. 2712 del c.c. non appare sufficiente a regolare la fattispecie in esame; sarebbe opportuno inserire nel Codice una disposizione specificamente dedicata all'efficacia probatoria del documento informatico non sottoscritto con alcun tipo di firma elettronica.

Tra l'altro, il fatto che l'art. 2712 faccia riferimento al disconoscimento piuttosto che al riconoscimento, ha indotto parte della dottrina alla singolare conclusione secondo cui, sotto il profilo dell'efficacia probatoria, "*potrebbe risultare preferibile il documento informatico privo di firma digitale, che non ha bisogno del riconoscimento della parte contro cui viene fatto valere per formare "piena prova", rispetto allo stesso documento munito di firma digitale, che in base al richiamo dell'art. 2702 c.c. necessita, per fare "piena prova" del riconoscimento della sottoscrizione da parte di colui contro il quale il documento è prodotto"*[207]. Spetterà ai giudici trovare una soluzione che, con tutta probabilità, si conformerà alla prassi di equiparare il riconoscimento (tacito, ex art. 215 c.p.c.) al mancato disconoscimento.

[206] Più esattamente in mancanza di contestazione della conformità ai fatti o alle cose rappresentate, non trattandosi di dimostrare l'imputabilità del documento, essendo privo di sottoscrizione.

[207] Patti S., *Efficacia probatoria del documento informatico*, in Bianca (a cura di), *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in *Nuove Leggi civ. comm.*, 2000, III-IV, 694.

Conclusioni

Giunti al termine di questo lavoro, va opportunamente osservato che le regole tecniche sulla firma digitale, esaminate in questa sede, potrebbero subire importanti cambiamenti per effetto della recente L. n. 69/09, recante "*disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile"*. La suddetta legge, all'art. 33, delega il Governo ad emanare un decreto legislativo per modificare il C.A.D. e prevede, tra gli obiettivi, anche quello di "*modificare la normativa in materia di firma digitale al fine di semplificarne l'adozione e l'uso da parte della pubblica amministrazione, dei cittadini e delle imprese, garantendo livelli di sicurezza non inferiori agli attuali*". Il rischio è che, nel momento in cui il Governo emenderà la normativa primaria in materia di firma digitale, le regole tecniche di cui sopra risultino già obsolete. Si ritiene auspicabile che in tale occasione ci si limiti a chiarire la normativa vigente e non si voglia, invece, sconvolgere il sistema con ulteriori innovazioni, che non farebbero altro che ingenerare confusione negli utilizzatori.

Sotto il profilo tecnico non si comprende, infatti, il senso di questa "semplificazione", visto che l'uso della firma digitale non presenta particolari difficoltà.

Per quanto riguarda il profilo della sicurezza, potrebbe risultare inutile e dispendioso introdurre nuove tecnologie[208], essendo quelle esistenti assolutamente affidabili.

Il punto sul quale si potrebbe intervenire attiene semmai alla terminologia utilizzata dal Codice per descrivere le diverse tipologie di firma: firma elettronica, firma qualificata, firma digitale. Dall'analisi finora compiuta appare evidente l'inutile previsione della firma qualificata, corrispondente tecnicamente alla firma digitale. Seppur l'espressione "digitale" appare più corretta sotto il profilo tecnico, è forse preferibile usare quella di "elettronica qualificata" che, ricollegandosi al certificato qualificato e al dispositivo sicuro per la creazione della firma, meglio si uniforma alla normativa comunitaria.

Sebbene sia necessaria una revisione del C.A.D., per approntare un sistema coerente e funzionale in sostituzione di una normativa indubbiamente contorta e faticosamente conciliabile con quella nazionale ed europea, non si può negare come il Codice si configuri, comunque, uno strumento normativo più adatto dei precedenti a disciplinare le esigenze di sicurezza e certezza legate alla formazione di documenti informatici ed alla relativa sottoscrizione elettronica.

A fronte di un sistema normativo completo, vi è però un sistema organizzativo che non consente l'applicazione dei principi contenuti nel Codice. La normativa sulla firma digitale, che intendeva garantire un risparmio di tempi e di costi attraverso la predisposizione di atti e documenti informatici, così da limitare gli adempimenti burocratici legati all'utilizzo del documento cartaceo, non ha prodotto gli effetti attesi.

[208] Ad esempio, la codifica mediante curve ellittiche, di cui si vocifera.

Dinanzi all'inadempienza delle amministrazioni la L. n. 69/09 ha previsto delle forme sanzionatorie, anche sotto forma di decurtazione di risorse finanziarie quantificate sulla base dei mancati risparmi derivati dall'inottemperanza alle disposizioni del Codice. Tra le altre misure che investono le P.A., meritano di essere menzionate quelle che prevedono: la diffusione delle applicazioni informatiche realizzate e dei servizi erogati con modalità digitali, nonché delle migliori pratiche tecnologiche e organizzative adottate[209]; l'implementazione del riuso dei programmi informatici[210]; l'obbligo dell'utilizzo delle procedure e delle reti informatiche nelle comunicazioni tra le P.A., con i loro dipendenti e con i concessionari di pubblici servizi; l'erogazione dei propri servizi, ove possibile, nelle forme informatiche e con le modalità telematiche.

Si intende, in tal modo, non solo facilitare al massimo i rapporti tra privati e la pubblica amministrazione, ma anche incentivare lo sviluppo del commercio elettronico, risultato questo in parte raggiunto, ma la cui completa realizzazione si avrà soltanto quando, sul piano legale, vi sarà la diffusa convinzione di poter fare affidamento su una "firma digitale sicura" .

Per realizzare questo scopo sarà necessario raggiungere l'equivalenza sostanziale e processuale fra la sottoscrizione cartacea e quella elettronica, nel solco di quanto già disposto dalla normativa europea.

È comunque presto per azzardare conclusioni definitive in merito alla riforma nel suo complesso. Bisognerà attendere che essa diventi effettivamente operativa, a seguito della riduzione del *digital divide*[211], dell'attuazione dei processi di semplificazione e razionalizzazione del sistema documentale e procedimentale e dell'entrata in funzione del nuovo Sistema Pubblico di Connettività[212] che colleghi tra loro gli uffici della Pubblica Amministrazione in un'unica grande rete.

Tale evoluzione si sta compiendo non solo per opera dell'intervento legislativo, ma anche per effetto di una nuova fiducia, contrapposta all'iniziale diffidenza, verso le nuove tecnologie. Il fenomeno "firma digitale" è, quindi, prima di tutto una sfida culturale, che va ben al di là di una mera innovazione tecnico-giuridica: è una vera e propria rivoluzione, che non può prescindere dalla formazione di una "coscienza digitale".

---

[209] Alla cui inadempienza si ricollegano sanzioni.

[210] Secondo quanto disposto dall'art. 69 del C.A.D.. Si richiede a tal fine che i programmi sviluppati per le P.A. presentino caratteri di modularità ed intersettorialità.

[211] Termine con il quale si indica il divario esistente tra le fasce della popolazione nell'accesso alle nuove tecnologie.

[212] Nell'art. 73 co. 2° del C.A.D., l' S.P.C. è definito come "*l'insieme di infrastrutture tecnologiche e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione*".

Bibliografia

Saggistica e Riviste

AA.VV., *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, a cura di Bianca, in *Nuove Leggi civ. comm.*, 2000, III-IV, 633.

AA.VV., *Diritto dell'Internet e delle nuove tecnologie telematiche*, a cura di Cassano G. e Cimino I. P., Cedam ed., 2009.

AA.VV., *Il Codice della pubblica amministrazione digitale: commento ragionato al Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche*, a cura di Quaranta M., Napoli, 2006.

BIANCA C. M., *La firma elettronica: si apre un nuovo capitolo*, in *Studium Iuris*, 2002, p. 1431.

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. 143.

CAMMARATA M., *Firme elettroniche, problemi normativi del documento informatico*, Monti & Ambrosini ed., 2007.

CARNELUTTI F., *Studi sulla sottoscrizione*, in *Riv. Dir. Comm.*, 1929, I. p. 509.

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. 35.

DUNI G., *Le firme elettroniche nel diritto vigente*, in *Dir. Informazione e Informatica*, 2006, 4-5, p. 501.

GRAZIOSI A., *La nuova efficacia probatoria del documento informatico*, in *Rivista trim. di dir. proc. civ.* , 2003, 01, p.53.

MINERVA M., *L'attività amministrativa in forma elettronica* , in *Foro. Amm.*, 1997, 04, 1300.

NEIROTTI L, *Riflessioni giuridiche sulla firma elettronica:limiti, problemi, prospettive*, in *Cyberspazio e diritto*, 2005, vol. 6, n. 3, p. 401.

PELOSI A., *Le nuove regole tecniche relative ai documenti informatici di cui al D.P.C.M. 13 gennaio 2004*, in *Contratti*, 2004, 8/9, p. 833.

PICCOLI P., ZANOLINI G., *Il documento elettronico e la firma digitale*, in *Riv. Notariato.*, 2000, n. 4, p. 879.

RODOTÀ, *Tecnopolitica, La democrazia delle nuove tecnologie della comunicazione*, La Terza 1997.

SANTANGELO E., NASTRI M., *Firme elettroniche e sigilli informatici*, in *Vita Notarile*, 2002, 2, p. 1118.

SARZANA DI SANT'IPPOLITO F., C*onsiderazioni in tema di documento informatico, firma digitale e regole tecniche*, in *Corriere Giuridico*, 1999, 7, p. 779.

SORRENTINO F., *La disciplina sulle firme elettroniche: ultimo tassello?*, in *Nuove Leggi Civ. Comm.*, 2003, 4-5, 801.

VINCENTI M., *Regole tecniche per la formazione, la trasmissione, la conservazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (D.P.C.M. 13 gennaio 2004)*, in *Archivio Civile*, 2004, 9, p. 999.

Sitografia

ALCEI (Associazione per la libertà nella comunicazione elettronica interattiva) in *http://www.alcei.it/index.php/archives/6.*

GIORDANO F., *Firma digitale: nuove regole per agevolare gli operatori*, in *http://icpressroom.wordpress.com/2009/07/02/firma-digitale-nuove-regole-per-agevolare-gli-operatori/.*

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

LISI A., ZINGARELLI S., *Commento al nuovo art. 2215 bis cod. civ.: "marcatura temporale" e "marca temporale"* , in *http://www.diritto.net/content/view/3750/6/.*

PATTI S., *L'efficacia probatoria dei "nuovi" documenti informatici* , in *http: /www.tribunaletrieste.it/documenti/relazioni/salvatore_patti.htm*, 2003.

SCACCIA R., *HSM, Hardware Security Module: la grande smart card*, in *http://geekinfosecurity.blogspot.com/2007/12/hsm-hardware-security-module-la-grande.html*

SILIPIGNI G., *La nuova marca temporale allunga la vita alla firma digitale*, 08/06/2009, in *http://www.nuovofiscooggi.it/attualita/articolo/la-nuova-marca-temporale-allunga-la-vita-alla-firma-digitale*.

***www.cnipa.gov.it* :**

C.N.I.P.A. – Ufficio Sicurezza, *Linee Guida per l'utilizzo della Firma Digitale*, in *http://www.cnipa.gov.it/site/_files/LineeGuidaFD_200405181.pdf*, Maggio 2004.

C.N.I.P.A.,*Guida alla Firma Digitale* , in *http://www.cnipa.gov.it/html/docs/GuidaFirmaDigitale2009_a.pdf*, Aprile 2009.

***www.interlex.it* :**

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

CAMMARATA M., *Firma digitale: gli errori da correggere*, in *http: //www.interlex.it/docdigit/.htm*, 24-09-2008.

MINERVA M., *Documento informatico e forma scritta*, in *http: //www.interlex.it/forum10/relazioni/30minerva.htm*, 08-06-2005.

***www.jei.it* :**

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.

Giurisprudenza

Sentenza Cass. Civ., 13 febbraio 1988, n. 1552, in *Vita Not.*, 1988; *Rep. Giur. It.*, 1988.

Sentenza Cass. Civ., Sez. I, 12 agosto 1997, n. 7530, in *Mass. Giust. Civ.*, 1997, p. 1408.

Sentenza Cass. Civ., 6/12/01, n. 11445, in *Rep. Foro It.*, 2001.

Sentenza Cass. Civ., 4/3/2004, n. 4395, in *Rep. Foro It.*, 2004.

Parere del Consiglio di Stato, 7 febbraio 2005, n. 11995, in *Giur. It.*, 2005, I, p. 1163.

Parere del Consiglio di Stato 30 gennaio 2006, n. 31, in *http://www.giurdanella.it/7296.*