**David D'Agostini**

# La firma digitale

(aggiornamento: 17 marzo 2005)

## 1. Introduzione.

La diffusione di elaboratori elettronici e di documenti non cartacei comporta (e comporterà sempre più in futuro) notevoli cambiamenti e nuove opportunità nel campo delle attività negoziali tra i privati e dei rapporti con la Pubblica Amministrazione.

Il passaggio dal documento cartaceo a quello informatico, quale espressione della volontà realizzata attraverso lo strumento elettronico, dà inevitabilmente vita a conseguenze giuridiche di notevole portata che l'ordinamento non ha potuto esimersi dall'affrontare; tra i problemi sui quali la dottrina si è già cimentata da oltre un decennio spicca il tema della rilevanza giuridica del documento elettronico.

A partire dal 1997[1] in Italia, una serie di provvedimenti normativi ha conferito valore giuridico al documento informatico e alla firma digitale.

Il legislatore nazionale ha dovuto ben presto fare i conti in primo luogo con le esigenze di coordinamento che hanno portato all'approvazione del Decreto del Presidente della Repubblica n.445/2000; successivamente con l'obbligo di recepimento della direttiva 1999/93/CE che è stata attuata mediante il Decreto Legislativo 23 gennaio 2002, n.10.

Allo stato attuale, è possibile sottoscrivere digitalmente un documento informatico e, purché ci si attenga alle norme vigenti, ottenere per esso piena validità legale.

Il processo legislativo ha anche fornito le indicazioni sulle tecnologie da impiegare per ottenere firme digitali che possano ritenersi equivalenti a quelle autografe; tali tecnologie, peraltro, sono in continua evoluzione per seguire esigenze sempre più complesse nella sottoscrizione digitale, nello scambio in rete e nella successiva gestione e conservazione dei documenti informatici.

Ma cosa si intende con tale espressione?

## 2. Il documento informatico.

[1] L. 15 marzo 1997, n.59 "*Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la rifoema della Pubblica Amministrazione e per la semplificazione amministrativa*" e D.P.R. 10 novembre 1997, n.513 "*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art.15, comma 2, della legge 15 marzo 1997, n.59*".

Il nostro ordinamento detta una serie di norme sul documento senza offrire, tuttavia, una nozione ampia e generale. La scienza giuridica si è interessata al concetto di documento intorno all'inizio del secolo scorso,[2] per giungere solo di recente a individuare le caratteristiche principali.[3]

Il documento, quale *cosa rappresentativa*, offre una rappresentazione di un fatto attraverso l'uso di un codice comunicativo comune sia all'autore sia al destinatario. Dal *genus* è isolata la *species* "documento scritto", con la distinzione codicistica tra atto pubblico (artt. 2699-2701 c.c.) e scrittura privata (artt. 2702-2708 c.c.). Anche se lo stato della tecnica e della documentazione erano limitate nel periodo in cui il codice venne emanato, le norme in materia sono state considerate suscettibili di interpretazione estensiva e di applicazione analogica.

Dagli anni sessanta la tecnica della documentazione si vale in misura sempre più crescente dell'informatica e consente la redazione di documenti attraverso elaboratori elettronici, denominati appunto, *documenti elettronici*. La dottrina più recente, attraverso uno scrupoloso esame degli elementi del documento scritto (individuati nella *dichiarazione* e nella *incorporazione in una realtà materiale*) ha stabilito una distinzione nella categoria del documento elettronico.

Si definisce documento elettronico *in senso stretto* l'atto memorizzato in forma digitale nella memoria di un elaboratore, senza la possibilità di essere letto o comunque percepito dall'uomo se non attraverso apposite macchine.

Si intende per documento elettronico *in senso ampio* ovvero *documento informatico* l'atto formato dall'elaboratore mediante le proprie "periferiche di uscita", non necessariamente in forma digitale, ma che può essere costituito da un testo alfanumerico, un disegno o un grafico riprodotti su un supporto cartaceo o, comunque, su un qualsiasi oggetto materiale senza la necessità di essere letto o percepito dall'uomo con l'ausilio di una apposita macchina traduttrice.

Il D.P.R. 445/00 definisce il documento informatico come "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

Nel corso degli ultimi anni, il legislatore ha attribuito rilevanza giuridica agli elaboratori elettronici ed alle tecniche di automazione. Esempi normativi sono presenti dal 1983 (l. n. 183, la quale introduce la macchina fac-simile nella trasmissione tra avvocati e procuratori di atti da produrre in giudizio). Di particolare rilevanza sono le norme in materia di atto amministrativo. L'art. 2 della l. 537/93 autorizza la conservazione e la esibizione di documenti "per finalità amministrative e probatorie" su "supporti ottici" conformi alle norme tecniche definite dall'Autorità per l'informatica nella pubblica amministrazione.

[2] F. Carnelutti, *La prova civile*, Cedam, Padova, 1915.

[3] G. Rognetta, *La firma digitale e il documento informatico*, Ed. Simone, 1999.

Anche nel campo penale si è avuto il riconoscimento del valore giuridico degli atti informatici. Il codice penale nell'art. 491bis, attraverso la novella del 1993 (l. n. 547), ha introdotto la nozione di documento informatico.

L'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 (nota anche come legge "Bassanini"), ha introdotto il fondamentale principio secondo cui "*gli atti, dati e documenti formati dalla pubblica amministrazione 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*".

## 3. Aspetti tecnici.

Così come per le informazioni su supporto cartaceo, anche per il documento informatico si prospetta la necessità di garantirne la sicurezza e la riservatezza nei confronti del destinatario.

La scienza moderna ha individuato nella "crittografia"[4] lo strumento adatto per conseguire queste utilità:

- *riservatezza* (protezione delle informazioni da accessi non autorizzati);
- *integrità* (garanzia che l'informazione non venga alterata);
- *autenticità* (identificazione certa del mittente).

La disciplina tecnica della c.d. firma digitale, definita dalla normativa statunitense come "sequenza di bit che il firmatario crea in relazione ad un messaggio chiaramente delimitato, sottoponendo il messaggio ad una funzione non invertibile, e successivamente crittando il messaggio risultante con un sistema asimmetrico di crittografia e la propria chiave privata", si fonda sulla scienza crittografica.

L'avvento del computer ha permesso di realizzare sistemi di crittografia di nuova concezione con chiavi di cifratura basate su principi materialmente impossibili da applicarsi con criteri manuali o meccanici. Un sistema di crittografia è essenzialmente un *algoritmo* che, può essere eseguito da un computer.

Esistono due classi principali di algoritmi che si basano sull'utilizzo di chiavi:

- algoritmi simmetrici (o a *chiave segreta o privata*) sono quelli usati dalla crittografia classica e permettono al mittente e al destinatario di usare la medesima chiave, rispettivamente, per crittare e decrittare un messaggio.
- algoritmi asimmetrici (o a *chiave pubblica*) si basano su una coppia di chiavi, una capace di cifrare, l'altra di decifrare l'informazione.

La tecnica della crittografia asimmetrica (o a chiave pubblica) sembra risolvere i problemi di "gestione" della chiave. Le debolezze del sistema a chiave segreta, derivanti dalla necessità di comunicare la chiave e dal suo ripetuto uso, sono superate.

Nel 1976 Whitfield Diffie e Martin Hellman pubblicarono uno studio su un sistema rivoluzionario per scambiare informazioni senza

[4] G. Ziccardi, *Crittografia e diritto*, Giappichelli, 2003.

preventivamente trasmettere la chiave segreta.

Nel 1978 venne costruito il primo crittosistema a chiave pubblica, RSA. Proposto dai ricercatori del Massachusetts Institute of Technology, Ron Rivest, Adi Shamir e Leonard Adleman; questo sistema di crittografia è attualmente il più diffuso.

La chiave con cui viene crittato il messaggio è differente da quella con cui esso viene decrittato in ricezione; il punto di forza su cui si basa l'algoritmo RSA è l'estrema difficoltà (matematica) di derivare la chiave segreta da quella pubblica. Questo tipo di cifrari trovano fondamento sulle funzioni unidirezionali. Si tratta di funzioni non invertibili (one-way), tali che il calcolo della funzione diretta sia semplice, mentre quello della chiave inversa si estremamente complesso. La funzione unidirezionale dell'RSA è costruita sfruttando la scomposizione in fattori primi dei numeri primi molto grandi.

I metodi crittografici a chiave pubblica possono essere utilizzati per la costruzione di strumenti per la firma digitale, variamente concepiti. Mentre nella crittografia la chiave pubblica viene usata per la cifratura, e il destinatario usa quella privata per leggere in chiaro il messaggio, nel sistema della firma digitale il mittente utilizza la funzione di cifratura e la sua chiave privata per generare un'informazione che (associata al messaggio) ne verifica la provenienza, grazie alla segretezza della chiave privata.

Chiunque può accertare la provenienza del messaggio utilizzando la chiave pubblica. L'algoritmo RSA, usato per generare firme elettroniche, si basa semplicemente sull'inversione del ruolo delle chiavi rispetto a quello utilizzato per assicurare la riservatezza. Le differenze fra le due applicazioni risiedono essenzialmente nel fatto che per la firma digitale si evita di dover applicare l'operazione di cifratura all'intero testo (con notevole risparmio di tempo).

Il testo da firmare viene compresso in una sorta di riassunto (detto *impronta digitale*), tramite un'apposita *funzione di Hash*, costruita in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta. La dimensione del riassunto è fissa, e molto più piccola di quella del messaggio originale; sicché la generazione della firma risulta estremamente rapida.

## 4. La sottoscrizione digitale.

Passando all'esame del processo di generazione della firma digitale,

questa viene apposta mediante una sequenza di tre operazioni.

Inizialmente si ha la generazione dell'impronta, mediante l'applicazione al testo da firmare di una funzione di hash appositamente studiata, la quale assicura l'unicità della sequenza di caratteri generata.

L'utilità dell'uso dell'impronta è duplice, in primo luogo consente di evitare che per la generazione della firma sia necessario applicare l'algoritmo di cifratura all'intero testo che può essere molto lungo. Inoltre permette l'autenticazione, da parte di una terza parte fidata (il certificatore), della sottoscrizione di un documento senza che questa venga a conoscenza del suo contenuto.

La generazione della firma consiste semplicemente nella cifratura, con la chiave segreta, dell'impronta digitale generata in precedenza. La firma digitale viene apposta al testo del messaggio, in una posizione predefinita (solitamente alla fine). Assieme alla firma vera e propria, viene eventualmente allegato anche il certificato da cui è possibile recuperare il valore della chiave pubblica.

L'operazione di verifica della firma digitale si effettua ricalcolando, con la medesima funzione di hash usata nella fase di sottoscrizione, il valore dell'impronta e controllando che il valore così ottenuto coincida con quello generato per decodifica della firma digitale stessa.

Qualora sia necessario attribuire ad un documento certezza circa il momento in cui questo è stato redatto ed è divenuto valido, si ricorre alla sua validazione temporale. Questa procedura (chiamata anche *time* stamping) consiste nella generazione da parte del certificatore di un'ulteriore marcatura digitale, che aggiunge all'impronta la data e l'ora.[5]

## 5. Il certificatore.

Il certificatore è definito come il soggetto che effettua la certificazione con lo scopo duplice di rendere certa l'identità del titolare del certificato e di instaurare con quest'ultimo un canale di comunicazione sicuro attraverso il quale vengono trasmesse le chiavi pubbliche.[6]

Mediante un software adatto al sistema crittografico adottato, l'utente genera una coppia di chiavi da utilizzare: una, che verrà mantenuta segreta, per l'apposizione della firma; l'altra, destinata alla verifica, che verrà resa pubblica attraverso i registri del certificatore. La certificazione della chiave pubblica ha lo scopo di assicurare, a chiunque riceva un documento correttamente firmato, l'identità del soggetto che ha posto la firma.

[5] Nella marca temporale sono contenute: data e ora di creazione, nome dell'emittente, impronta del documento.

[6] E. Tosi, *I problemi giuridici di Internet*, Giuffrè, 2001.

Una volta emesso, il certificato viene reso disponibile in uno o più registri, ai quali può accedere chiunque abbia bisogno di verificare la validità di una sottoscrizione digitale.

L'utente dispone, da questo momento, della sua chiave privata con la quale firmerà i messaggi; della chiave pubblica indicata nei registri o inviabile direttamente al destinatario come allegato del messaggio; del certificato che attribuisce alla firma validità e provenienza.

L'attività dei certificatori (che si dividono in qualificati e accreditati) è libera e non necessita di autorizzazione preventiva; il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento:

α) sull'esattezza e sulla completezza dei dati contenuti alla data del rilascio;

β) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma;

Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato, salvo che provi d'aver agito senza colpa.

Il certificatore può indicare, in un certificato qualificato, i limiti d'uso di detto certificato ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso; in tal caso non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

## 6. Verificazione e querela di falso.

La scrittura privata ha efficacia di piena prova al verificarsi, alternativamente, di quattro ipotesi:

1) il riconoscimento espresso (da parte del firmatario – art. 2702 c.c.);
2) il riconoscimento tacito (quando la persona che risulta avere apposto la sottoscrizione non la disconosce entro i termini previsti – art. 215 c.p.c.);
3) il riconoscimento legale (ottenuto con l'autenticazione della sottoscrizione da parte del notaio o di altro pubblico ufficiale autorizzato – art. 2703 c.c.);

4) il riconoscimento guidiziale (attribuito dalla decisione del giudizio di verificazione, a seguito di incidente istruttorio ovvero in via principale – art. 216 c.p.c.).

La piena efficacia raggiunta dal mezzo di prova documentale può essere inficiata attraverso uno specifico procedimento: il giudizio di falso (art. 221 c.p.c.).

La dottrina discute se la querela di falso sia ammissibile solo nei confronti di una scrittura riconosciuta o legalmente considerata come riconosciuta, ovvero anche nei confronti di scrittura non riconosciuta. A differenza del giudizio di verificazione, il cui oggetto è l'accertamento dell'autenticità della scrittura privata al fine di attribuirne la paternità al soggetto che l'ha disconosciuta, la querela di falso verifica la verità del documento. Il giudizio di verificazione, attraverso lo studio comparativo delle scritture, si pone l'obiettivo di individuare l'autenticità del documento attribuendone la paternità ad un determinato soggetto. Il giudizio di falso, prescindendo dall'esame della forma del mezzo di prova, è volto ad accertare la provenienza delle dichiarazioni contenute nella scrittura privata; il procedimento ha per oggetto il fatto della dichiarazione contenuta nell'atto.

La scrittura privata informatica è sottoposta alle medesime regole descritte dall'art. 2702 c.c., ma le modalità tecniche della firma digitale, e in particolare del procedimento di verifica della scrittura, permettono la conoscibilità dell'autore del documento da parte del destinatario producendo conseguenze sugli istituti della verificazione e giudiziale e della querela di falso, oggetto d'interesse degli studiosi della materia.

Un filone di interpretazione, denominabile "*riformatore*", considera la firma digitale come una rottura con il vecchio sistema di imputazione degli atti giuridici. Non essendoci continuità, i procedimenti di verifica dell'autenticità del documento (giudizio di verificazione) e della dichiarazione (querela di falso) subiscono modifiche. Così come descritto dal regolamento, il documento informatico provvisto di firma digitale produce l'inapplicabilità dell'istituto della verificazione delle prove documentali.

A tale teoria si contrappone la dottrina "*conservatrice*" che interpreta la firma digitale come un diverso sistema di imputazione degli atti giuridici, la quale, tuttavia, non determina un conflitto con il sistema della firma autografa. Il giudizio di verificazione e la querela di falso continuano, pertanto, a svolgere la loro originaria funzione.

## 7. Le firme elettroniche.

Il Testo Unico sulla documentazione amministrativa (vale a dire il D.P.R. 445/00 come modificato dal d.lgs.10/02[7] e dal D.P.R. 137/03[8]) introduce il più ampio concetto di firma elettronica.

L'impostazione di fondo della nuova disciplina improntata alla "neutralità tecnologica" è orientata alla liberalizzazione dell'uso delle firme elettroniche e al riconoscimento della validità anche a

[7] Decreto legislativo 23 gennaio 2002, n. 10 "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche".

[8] Decreto del Presidente della Repubblica 7 aprile 2003 n. 137 "*Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del D.Lgs. 23 gennaio 2002, n. 10*".

firme dotate di uno standard tecnico meno sicuro rispetto alla firma digitale; quest'ultima, pertanto, si configura come una *species* all'interno dell'ampio *genus* delle firme elettroniche.

Il sistema di firme attualmente in vigore distingue tra le seguenti categorie:

1) la firma elettronica cd. "*debole*", definita come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 2, lett. a, d.lgs. 10/2002);
2) la firma elettronica *avanzata*, definita come la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 2, lett. g, d.lgs. 10/2002);
3) la firma elettronica avanzata basata su un certificato qualificato e generata attraverso un dispositivo di firma sicura (art. 6 d.lgs. 10/2002);
4) la firma elettronica sicura ovvero la firma digitale adottata in Italia con il d.P.R. 513/1997.

## 8. La firma elettronica "semplice": forma scritta ed efficacia probatoria.

Il documento sottoscritto con la firma elettronica soddisfa il requisito legale della forma scritta ed è liberamente valutabile dal giudice secondo le caratteristiche di oggettività e sicurezza.

Esso soddisfa comunque l'obbligo previsto dagli artt. 2214 e segg. c.c., relativi alla tenuta delle scritture contabili, e da ogni altra analoga disposizione legislativa o regolamentare. In ogni caso - stabilisce l'art. 10, comma 4 - al documento informatico, sottoscritto con firma elettronica, non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica.

La soluzione adottata prima del recepimento della direttiva permetteva di equiparare il documento informatico sottoscritto con firma digitale alla scrittura privata sul piano della forma, oltreché sul piano della prova, consentendo di compiere in forma informatica tutti gli atti per i quali è richiesta una forma scritta *ad susbstantiam* (per es. quelli previsti dall'art 1350 c.c.). Peraltro l'uso della firma digitale permetteva agevolmente di considerare pienamente realizzata anche la funzione probatoria del documento.

In nessun caso si riteneva che un documento informatico senza firma digitale o con firma

elettronica semplice potesse integrare il requisito della forma scritta.

La disciplina di recepimento della direttiva attua invece un'inversione di tendenza, attribuendo anche alla firma elettronica semplice questa duplice forza (di esistenza dell'atto e probatoria).

Alla firma elettronica semplice non viene riconosciuta l’efficacia probatoria della scrittura privata ex art. 2702 c.c. tipica dei documenti sottoscritti, bensì quella prevista dall'art. 2712 c.c. riguardo ai fatti e alle cose rappresentate.

L'assenza di una chiara definizione degli effetti imputabili alla firma elettronica si riflette anche sugli impatti che quest'ultimo istituto può avere sulla dinamica delle prove.