DOCUMENTO INFORMATICO, FIRMA DIGITALE E FIRME ELETTRONICHE

1) NOZIONI GIURIDICHE PRELIMINARI

Al fine di poter comprendere la disciplina relativa ai documenti informatici, alle firme digitali ed elettroniche, soprattutto in riferimento al loro valore legale, e' necessario accennare ad alcuni termini giuridici fondamentali.

a) DOCUMENTO

Non esiste una definizione legislativa di documento, il quale però è generalmente considerato come una "*res*, ovvero come qualsiasi cosa idonea a rappresentare e far conoscere un fatto: il testimone è persona che narra e il documento è cosa che rappresenta. Per avere immediata percezione delle finalità del documento basta pensare all'etimo latino "*docere"*: il documento è, dunque, qualcosa destinato a *docere,* insegnare, dimostrare. Nel linguaggio informatico il documento indica, di solito, i *files* di contenuti (per esempio di *Word).* Più precisamente, il documento è una "*res signata*", cioè un oggetto che reca una serie di segni tracciati direttamente dall'uomo o da apparati predisposti dall'uomo, volti a conferirgli portata rappresentativa.

Da un punto di vista legale il documento è destinato a produrre effetti giuridici diversi a seconda dei requisiti che possiede: per fare un esempio, una banconota o un assegno sono entrambi documenti ed entrambi possono essere utilizzati come mezzi di pagamento, ma hanno requisiti diversi ai fini della loro validità : l'assegno è valido e produce effetti giuridici solo se è dotato della sottoscrizione autografa di chi lo

emette, mentre la banconota è valida se presenta determinate caratteristiche fisiche (un particolare tipo di stampa e di carta, una ben definita serie di informazioni) che certificano la sua corrispondenza a un determinato valore.

b) **FIRMA AUTOGRAFA**

Dal punto di vista materiale si tratta di un segno apposto manualmente da un soggetto su un supporto contenente informazioni. La sua funzione principale è quella di essere ricollegabile in maniera univoca al soggetto che l'ha apposta, essendo quasi impossibile che due soggetti diversi firmino esattamente allo stesso modo. Non esiste una definizione leagle di firma, perché il codice civile si occupa solamente di disciplinare gli effetti giuridici di un documento sottoscritto, effetti che possono sinteticamente essere riassunti come segue.

1) **Identificazione dell'autore del documento**;
2) **paternità del documento**: con la sottoscrizione l'autore del documento si assume la paternità dello stesso anche in relazione al suo contenuto; a questo proposito si parla di non ripudiabilità del documento sottoscritto;
3) **integrità del documento**: il documento scritto e sottoscritto manualmente garantisce, o almeno in teoria dovrebbe farlo, da alterazioni materiali da parte di persone diverse da quella che lo ha posto in essere.

c) SCRITTURA PRIVATA

Nel nostro ordimanemto statale, per poter concludere validamente un contratto, non è in genere richiesto l'uso della forma scritta, per cui un contratto può essere validamente concluso anche oralmente: tuttavia, per i contratti ritenuti più importanti

è imposto l'uso della forma scritta, che assume due diverse forme: scrittura privata e atto pubblico.

L'art. 2702 del codice civile si occupa del valore probatorio della scrittura privata la quale, identificando l'autore del documento, garantisce che questo provenga da chi lo ha sottoscritto; in particolare, l'articolo 2702 del codice civile dispone che " *la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni in esso contenute*". Questo valore probatorio privilegiato, tuttavia, sussiste solo se la firma non sia stata disconosciuta dal suo presunto autore o, alternativamente, se la firma sia stata autenticata da un notaio o da altro Pubblico Ufficiale autorizzato dalla legge

Potrebbe tuttavia accadere che, pur essendo in presenza di una scrittura privata con sottoscrizione non disconosciuta o comunque autenticata da un Pubblico Ufficiale, si ponga un problema di alterazione materiale del documento e che pertanto l'autore contesti la falsità materiale del documento medesimo e non della firma che vi ha apposto; in questo caso, l'unico modo per togliere valore probatorio al documento scritto e sottoscritto (non disconosciuto o autenticato) è quello di dimostrare che si tratta di un falso, attaverso una complesa procedura civilistica che prende il nome di querela di falso: tipico è il caso di documenti contraffatti successivamente alla sottoscrizione.

d) SCRITTURA PRIVATA AUTENTICATA

La sottoscrizione avviene in presenza di un notaio o altro Pubblico Ufficiale a ciò autorizzato dalla legge.

e) ATTO PUBBLICO

E’ l’atto formato da un notaio o altro Pubblico Ufficiale autorizzato ad attribuirgli pubblica fede nel luogo in cui è formato. A differenza della scrittura privata, l’atto pubblico è materialmente redatto dal notaio e fa piena prova, fino a querela di falso, non solo della provenienza del documento da parte del Pubblico Ufficiale che lo ha formato, ma anche delle dichiarazioni che le parti hanno reso in sua presenza: l'atto pubblico non prova la veridicità di quanto attestato dalle parti, ma solo che le parti stesse hanno reso tali dichiarazioni.

f) FALSO IDEOLOGICO E FALSO MATERIALE

In maniera molto sintetica si può dire che il falso materiale individua un documento **non genuino**, in quanto materialmente redatto da una persona diversa da quella che apparentemente risulta dalla firma, o semplicemente alterato nel suo contenuto con aggiunte o cancellazioni, o mediante l’apposizione di una firma falsa. Il falso ideologico, invece, individua un documento materialmente non alterato, ma il cui contenuto **non è veritiero**.

g) DOCUMENTO INFORMATICO

Per la prima volta il termine viene utilizzato dal legislatore italiano nel 1993, quando è stata introdotta in Italia la disciplina dei *computers crimes*, che costituirà oggetto di una separata trattazione. In questa sede interessa solo evidenziare che per documento informatico si intendeva “*qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli*”. Si tratta di una definizione estremamente generica, che non chiarisce affatto che cosa debba intendersi, da un punto di vista tecnico e pratico, per documento informatico. Il quadro normativo e giurisprudenziale è stato frammentario

e disorganico sino all'emanazione del **dpr n. 513 del 1997** che ha riconosciuto validità agli atti informatici e alla firma digitale.

2) LA LEGISLAZIONE SULLA FIRMA DIGITALE

In materia di firma digitale e documento informatico esiste un doppio canale di legislazione : uno di origine italiana e uno di origine comunitaria. Originariamente, infatti, esisteva solo la disciplina italiana sulle firme digitali: **la legge n. 59 del 1997** con il proprio regolamento di attuazione contenuto nel **dpr n. 513 del 1997**, che è poi stato interamente sostituito dal **dpr n. 445 del 2000** . Importante è altresì il **decreto della Presidenza del Consiglio dei Ministri del 1999 (dpcm),** che disciplina gli aspetti tecnici della firma digitale. Anche questo decreto è stato recentemente modificato alla luce delle novità normative in tema di firme elettroniche: le nuove regole tecniche sono state decretate dal **Consiglio dei Ministri in data 13 gennaio 2004**. La normativa italiana sulla firma digitale è dunque articolata su tre livelli:

- legge n. 59 del 1997;
- il Decreto di attuazione n. 513 del 1997 poi confluito nel decreto n. 445 del 2000;
- il Decreto Presidenziale del febbraio 1999, modificato ed integrato dal dpcm del 13 gennaio 2004.

Successivamente la materia è stata disciplinata anche a livello europeo con la **Direttiva 1999\93\CE**, che poi è stata recepita in Italia con il **decreto legislativo n. 10 del 23 gennaio 2002** e con il regolamento di attuazione contenuto nel **dpr n. 137**

del 7 aprile 2003. In particolare, il dpr n. 137 del 2003 coordina la disciplina europea con quella italiana. La normativa europea, infatti, ha disciplinato le cosiddette firme elettroniche che, come vedremo successivamente, stanno in un rapporto di *genus a species* con la firma digitale. In estrema sintesi possiamo quindi dire che attualmente esiste una disciplina generale sulle varie tipologie di firme elettroniche, ivi compresa, come *species* particolare, la firma digitale.

Recentissimamente è intervenuta un' ulteriore modifica normativa: si tratta del **Codice dell'Amministrazione digitale** introdotto con il Decreto legislativo n. 82 del 2005, che costituisce il risultato finale di tutte le precedenti stratificazioni normative. Passiamo ora ad analizzare la disciplina sulla firma digitale.

2.1 LA DISCIPLINA ITALIANA SULLA FIRMA DIGITALE

Con la legge n. 59 del 1997, che si occupa della semplificazione dell'attività della pubblica amministrazione, è stato per la prima volta introdotto nell'ordinamento italiano il principio generale della validità e della rilevanza giuridica delle rappresentazioni informatiche. Infatti l'articolo 15 dispone che *"gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonchè la loro trasmissione e archiviazione, sono validi e rilevanti a tutti gli effetti di legge"*.

L'esigenza di riconoscere piena validità ai documenti informatici nacque unicamente per garantire alla pubblica amministrazione la possibilità di trasmettere atti giuridici in rete; tuttavia l'ambito di applicazione della disposizione è generale perché si riferisce esplicitamente anche ai documenti informatici privati.

L'articolo 15 sopra richiamato rimanda ad un successivo regolamento di attuazione la disciplina specifica relativa ai criteri e alle modalità di formazione, archiviazione e trasmissione del documento con strumenti informatici e telematici: si tratta del dpr n. 513 del 1997, il quale stabilisce e disciplina in concreto il documento informatico. Questo regolamento è stato poi successivamente abrogato e tutte le disposizioni di legge in esso contenute sono state unificate ad altri due regolamenti e sono confluite nel dpr n. 445 del 2000, detto anche **testo Unico della Pubblica Amministrazione**. Ricordiamo ancora una volta che oggi tutta la materia è regolata dal nuovo **Codice dell'Amministrazione digitale.**

Il documento informatico viene definito dall'art. 1 del dpr n 445 del 2000 come "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".* La vera portata innovativa della legge del 1997 e dei due regolamenti di attuazione, tuttavia, è quella di aver consentito la possibilità di **firmare digitalmente** un documento informatico con il sistema "crittografico" delle chiavi asimmetriche e di attribuire ad un documento firmato con queste modalità il valore di una scrittura privata.

Con la tecnologia della crittografia si riesce a garantire **la provenienza e l'integrità** del documento informatico. Infatti, nella definizione di firma digitale fornita dall'art 1 lett n) del dpr n 445 del 2000, ci si riferisce ad una procedura capace di rendere manifesta e di verificare la provenienza e l'integrità del documento.

La crittografia è una scienza matematica che consente di costruire un sistema attraverso il quale sia possibile cifrare un testo così da impedirne la lettura a soggetti diversi dal mittente e dal destinatario, con un certo grado di attendibilità. La crittografia non è certo una novità: i procedimenti di cifratura esistono fin

dall'antichità e venivano utilizzati per proteggere i documenti che dovevano essere mantenuti segreti. Gli esempi storici sono numerosi: Giulio Cesare, durante le battaglie in Gallia, mandava messaggi segreti usando come tecnica quella di sostituire ogni parola con quella successiva in ordine alfabetico; i banchieri fiorentini nel Medio Evo utilizzavano tecniche crittografiche per proteggere le proprie lettere di credito inviate alle loro file decifrare il testo e quindi iali; le macchine "Enigma" utilizzate dai tedeschi durante la seconda guerra mondiale utilizzavano tecniche crittografiche.

L'obiettivo di chi cripta un messaggio è quello di tradurre il linguaggio del testo in chiaro in un nuovo linguaggio che non possa essere compreso da altri se non in presenza di una chiave capace di rendere nuovamente il testo in chiaro. Il fondamentale problema di tutti i metodi della crittografia è quello dello scambio della chiave, ovvero dell'accordo con il destinatario del messaggio su quale codice usare per cifrare e decodificare il messaggio. Nei sistemi crittografici tradizionali la stessa chiave serve per cifrare e decifrare il testo e quindi iali; le macchine "Enigma" utilizzate dai tedeschi durante la seconda guerra mondiale utilizzavano tecniche crittografiche.

è necessario comunicare al destinatario la chiave stessa: si tratta della cosiddetta **crittografia simmetrica**, che presenta molti svantaggi in ordine alla sicurezza delle comunicazioni. La possibilità che la chiave venga intercettata ha infatti ostacolato il diffondersi di questo metodo e si è così passati alla più sicura **crittografia asimmetrica:** in questo sistema vengono usate due chiavi diverse e univocamente correlate: conoscendo una delle due chiavi non è possibile risalire all'altra; si cifra il

documento con una delle dè necessario comunicare al destinatario la chiave stessa: si tratta della cosiddetta **crittografia simmetrica**, che presenta molti svantaggi in ordine alla sicurezza delle comunicazioni. La possibilità che la chiave venga intercettata ha infatti ostacolato il diffondersi di questo metodo e si è così passati alla più sicura **crittografia asimmetrica**; in questo sistema vengono usate due chiavi diverse e univocamente correlate: conoscendo una delle due chiavi non è possibile risalire all'altra; si cifra il documento con una delle due chiavi, mentre per decodificarlo si usa l'altra. Non è dunque necessario comunicare al destinatario la propria chiave e con ciò si evitano i rischi della circolazione della chiave stessa. Ognuna delle chiavi può sbloccare il codice apposto dall'altra e soltanto questo: se una è usata per la cifratura del documento, l'altra sarà impiegata per decifrarlo e viceversa. Partendo da questo sistema è nato il PGP (dal nome dell'inventore Phil Zimmermann), sistema che consente di generare una coppia di chiavi, rendendone una pubblica e tenendo l'altra segreta. Il legislatore italiano ha adottato il sistema della crittografia a chiavi asimmetriche.

L'articolo 1 del dpr n. 513 del 1997 definisce la firma digitale come il **"risultato della procedura informatica (validazione), basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore, tramite la chiave privata e al destinatario tramite quella pubblica, rispettivamente di rendere manifesta e verificare provenienza e integrità di un documento informatico o di un insieme di documenti informatici**". I requisiti tecnici del documento informatico sono stati fissati dal decreto della Presidenza del Consiglio dei Ministri (di seguito indicato come dpcm) dell'8 febbraio 1999. In

particolare, l'articolo 5 del dpcm dispone che" **la generazione della coppia di chiavi deve essere effettuata mediante apparati e procedure che assicurino, in rapporto allo stato di conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia di chiavi, nonché la segretezza della chiave privata".** Quest'ultima, dunque, è il mezzo attraverso il quale il titolare firma il documento informatico facendo in modo che sia a lui riconducibile. Al fine di mantenere la segretezza della chiave privata è anche possibile ottenerne il deposito presso un notaio, nelle forme previste per il deposito dei testamenti olografi.

La chiave pubblica, invece, serve per decifrare il documento firmato con la corrispondente chiave privata e per la sua naturale destinazione deve essere portata a conoscenza di tutti i destinatari del documento, in modo che sia possibile leggerlo ed assicurarsi della provenienza del medesimo. In estrema sintesi, **la firma digitale si genera applicando la propria chiave privata al testo, mentre il destinatario decifra il testo con la chiave pubblica del mittente e, se i due testi risultano uguali, ottiene la (presumibile) certezza dell'identità del mittente e dell'integrità del documento**.

Il processo di decifrazione, infatti, consente di verificare con un accettabile grado di certezza, **la provenienza** e **l'integrità** della dichiarazione pervenuta. Infatti, se il documento non fosse firmato con la chiave privata del mittente, non sarebbe decifrabile con la chiave pubblica del destinatario. Per ciò che attiene, invece, al profilo dell'integrità del documento trasmesso, occorre tenere presente che la firma digitale non è apposta in calce al documento essendo, al contrario, un algoritmo grazie al quale viene cifrato tutto il documento nella sua interezza e quindi tutto il

documento è firmato dal suo autore. Non è possibile modificare nessuna parola (*byte*), senza incidere sulla firma di tutto il documento. Per la verità, considerato che per cifrare e decifrare tutto il documento occorrerebbe molto tempo, si ricorre a una scorciatoia che consiste nel cifrare solo un brevissimo riassunto del testo stesso, ottenuto con una procedura detta *funzione di hash;* se, alla fine della procedura, l'impronta che risulta dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la funzione di *hash* al testo chiaro, vuol dire che esso proviene da chi appare come il titolare della chiave pubblica e che non è stato alterato dopo la generazione della firma digitale. In questo modo si riesce anche a scongiurare il pericolo di manomissioni del documento e, quindi, eventuali falsi materiali. In sintesi, il sistema della firma digitale soddisfa il requisito della forma scritta, in quanto assicura la provenienza, la paternità e l'integrità del documento. Si pone però un problema: come può il destinatario del documento essere sicuro che la chiave pubblica che impiega per verificare la firma del mittente (A) sia effettivamente di A e non di un altro che si fa passare per lui? Occorre qualcuno, una terza persona fidata, che certifichi che quella chiave pubblica appartiene veramente a quel soggetto e non ad un altro. A questo proposito, il dpr del 1997 prevede che una delle due chiavi asimmetriche sia resa pubblica mediante un'apposita procedura, detta di certificazione, che garantisca l'associazione tra la coppia di chiavi e il soggetto sottoscrittore. Nel certificato possono, eventualmente, essere anche indicati eventuali poteri di rappresentanza, l'esercizio congiunto della coppia di chiavi etc. Il certificatore cura poi la custodia delle chiavi pubbliche per un periodo non inferiore a dieci anni e provvede a revocare o sospendere il certificato nei casi previsti dal

regolamento, procedendo alla relativa pubblicazione. La revoca o la sospensione del certificato possono aversi nei casi di sottrazione o smarrimento del dispositivo di firma e, in genere, in tutti i casi di perdita di riservatezza della chiave privata e devono essere pubblicate in tempi molto stretti per evitare di trarre in inganno chi riceve un documento informatico e verifica come valida una firma digitale che invece non lo è più. Il certificatore che intenda cessare l'attività deve darne notizia almeno sei mesi prima ai titolari e alle Autorità di controllo e i certificati validi possono essere passati a un altro certificatore o definitivamente revocati.

In sintesi, la firma digitale si fonda sui seguenti elementi:

- sistema crittografico delle chiavi asimmetriche;

- cifratura del documento mediante la funzione di *hash*;

- **presenza di un soggetto, certificatore, che garantisce la corrispondenza tra il titolare della coppia di chiavi e un determinato soggetto attraverso un certificato che viene reso pubblico e consultabile *on-line*.**

Un' ultima considerazione: utilizzando il sistema delle doppie chiavi anche al contrario, è possibile altresì garantire la segretezza del documento trasmesso. Infatti, il documento firmato con firma digitale può essere letto da chiunque, in considerazione della pubblicità della chiave che serve per decifrare il documento. Se, invece, il mittente provvede a firmare il documento anche con la chiave pubblica del destinatario, sarà solo quest'ultimo in grado di decifrare il documento con la relativa chiave privata corrispondente. Naturalmente, in questo caso, entrambi i soggetti devono possedere una coppia di chiavi per la generazione di firme digitali.

2.2 LA NORMATIVA EUROPEA

Il decreto legislativo n. 10 del 23 gennaio del 2002 ha recepito la Direttiva Europea 1999\93 sulle firme elettroniche. Successivamente è stato emanato un regolamento di attuazione che coordina la nuova normativa europea con quella italiana precedente contenuta nel regolamento n 445 del 2000: tale regolamento è contenuto nel **dpr n. 137 del 7 aprile 2003**, entrato in vigore nel giugno del 2003. Questo decreto coordina, dunque, due normative di origine diversa: una italiana e una comunitaria. Ricordo ancora una volta che attualmente tutta la disciplina in questione è confluita nel recente Codice dell'Amministrazione digitale.

Il concetto di firma elettronica, come abbiamo già anticipato, non è uguale a quello di firma digitale, designando la prima un *genus* e la seconda una *species:* per firma elettronica si intende il risultato dell'applicazione, a un messaggio in formato digitale, di una tecnologia, tra le tante possibili, che consenta di attribuire al messaggio alcune funzioni della sottoscrizione autografa. Possono infatti essere utilizzati metodi diversi per l'applicazione delle firme elettroniche: codici di identificazione personale o chiavi biometriche. I metodi di classificazione per l'autenticazione delle firme elettroniche possono essere classificati in : "*something you are*", "*something you have*" e " *something you know*", a seconda che il meccanismo di autenticazione si basi sulle conoscenze dell'utente (conoscenza di una parola chiave), sulle caratteristiche fisiche (impronta digitale o della retina) o sul possesso di un oggetto (tesserina magnetica). A seconda delle tecniche utilizzate le firme elettroniche possono o meno essere in grado di garantire, al pari della firma digitale, **integrità** e **provenienza** dei dati. In particolare, la firma elettronica viene

definita dalla legge come "insieme di dati in forma elettronica, allegati o connessi tramite associazione logica ad altri dati elettronici, utilizzati con metodo di autenticazione informatica".

L'espressione firma digitale indica, per contro, uno specifico tipo di firma elettronica, che utilizza il sistema della crittografia.

La firma elettronica non implica l'utilizo di una specifica tecnologia, quella digitale fa invece riferimento alla crittografia a chiave asimmetrica

Il decreto n. 137 del 2003 prima e il Codice dell'Amministrazione digitale, successivamante, coordinano le due tipologie di firma informatica, dando vita a diversi tipi di firma: **firma digitale**, **firma elettronica qualificata (o forte) e firma elettronica semplice (o debole)**. Si prevede anche una diversa disciplina dei certificatori, perché si passa da un sistema di monopolio ad un sistema di liberalizzazione dell'attività dei certificatori.

A questo punto, passiamo ad analizzare il valore giuridico del documento informatico alla luce della nuova normativa europea.

3 IL VALORE GIURIDICOI DEI DOCUMENTI INFORMATICI

I documenti informatici hanno una diversa efficacia giuridica a seconda del tipo di firma elettronica che viene utilizzato. Si possono dunque prospettare le seguenti ipotesi:

a) il documento informatico è sprovvisto di qualsiasi firma elettronica ed ha la stessa efficacia probatoria delle riproduzioni meccaniche disciplinate dall'art 2712 del codice civile; questa disposizione prevede che " le riproduzioni fotografiche o

cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti o di cose formano piena prova dei fatti e della cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime";

b) il documento informatico sottoscritto con firma elettronica semplice o debole è liberamente valutabile dal giudice ai sensi dell'articolo 116 del codice di procedura civile. Si tratta di tutti quei sistemi che in vario modo possono permettere di individuare un soggetto in base alle sue conoscenze (PIN, password e *user name*), oppure a caratteristiche fisiche (impronte digitali o della retina) oppure, infine, in base al possesso di una *smart card*. La valutazione dell'efficacia probatoria di tali documenti è interamente rimessa alla decisione del giudice, il quale non è vincolato ad attribuire a tali documenti alcun valore probatorio pur in assenza di disconoscimentio della parte contro cui sono prodotti e, per contro, potrebbe decidere d'ufficio per l'attendibilità degli stessi pur in presenza di contestazioni. Esemplificando, non sarà più possibile dubitare che una transazione commerciale possa essere provata esibendo al giudice la traccia elettronica o cartacea di un bancomat, fermo restando il potere del giudice stesso di ritenere o meno attendibile una tale prova.

c) Documento informatico munito di firma digitale o di firma elettronica qualificata. Con l'espressione "firma elettronica qualificata" non ci si riferisce ad una tecnologia ben precisa, perché la Direttiva Europea si limita a prevedere una sorta di protocollo di sicurezza delle firme elettroniche costituito dalle tre unità:**firma elettronica qualificata, certificato qualificato** e **dispositivo di firma sicura**.

Quindi, qualunque firma si dimostri rispettosa di questi tre requisiti avrà la stessa validità ed efficacia probatoria della firma digitale e, dunque, farà piena prova della provenienza delle dichiarazioni in esso contenute, fino a querela di falso. Un'efficacia probatoria così intensa, tuttavia, potrà essere attribuita solo dopo che un apposito Dipartimento istituito presso la Presidenza del Consiglio dei Ministri abbia controllato la rispondenza del prodotto informatico e del soggetto che chiede di commercializzarlo al grado di sicurezza richiesto.

Il documento munito di firma digitale o di firma elettronica qualificata ha dunque la stessa efficacia della scrittura privata. Anzi, a ben vedere, ha un'efficacia probatoria maggiore rispetto a quella della scrittura privata. Ricordiamo, infatti, che la scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni in essa contenute, solo se sussiste, alternativamente, uno tra i requisiti previsti dall'art 2702 del codice civile, ovvero il mancato disconoscimento o l'autenticazione del notaio. Il documento informatico munito di firma digitale o firma elettronica avanzata sembrerebbe in realtà non disconoscibile; a ben vedere, infatti, mentre per verificare la firma apposta su un foglio è necessario procedere ad un esame grafologico per dimostrare che la sottoscrizione è autografa ed accertarne, quindi, la provenienza dal soggetto che si suppone averla apposta, nel caso di documento informatico sottoscritto con firma digitale basta verificare la corrispondenza della firma con la chiave pubblica del presunto sottoscrittore per accertarne la provenienza da quest'ultimo; conseguentemente, il disconoscimento della firma digitale sarebbe precluso, perché con la semplice prova della corrispondenza tra la chiave pubblica e la chiave privata utilizzate vengono accertate

sia la provenienza del documento che l'assenza di alterazioni del medesimo; l'unica ipotesi di falsità materiale che può configurarsi (atteso che le alterazioni materiali del documento sono da escludere grazie alla funzione di *hash*), è che la firma sia apposta da persona diversa dal legittimo proprietario del dispositivo di firma. Di conseguenza, l'oggetto del disconoscimento non sarà relativo alla firma ma all'effettivo utilizzo della firma digitale da parte del titolare. Il concetto di falsità materiale non sarà più dunque riferibile, in linea di massima, alla paternità della firma, quanto piuttosto a quello di responsabilità nel custodire il dispositivo di firma.

4)BREVE QUADO DI SINTESI

Le varie fattispecie di documento informatico possono così essere sinteticamente riassunte:

1) documento informatico sottoscritto con firma digitale avente valore di piena prova della provenienza delle dichiarazioni in esso contenute fino a querela di falso. Si tratta del documento informatico già originariamente disciplinato dal dpr n. 513 del 1997 e, dopo, dal dpr n. 445 del 2000;

2) documento informatico sottoscritto con firma elettronica qualificata, avente la stessa efficacia probatoria della firma digitale. Occorre, ai fini di una così intensa efficacia probatoria, oltre alla **firma elettronica qualificata**, il **certificato qualificato** e il **dispositivo per la creazione della firma sicura**;

3) documento informatico sottoscritto con firma elettronica semplice, liberamente valutabile dal giudice. In tale caso rientrano sia i documenti informatici sottoscritti con un sistema di riconoscimento ove non sia prevista la figura del certificatore, sia i casi in cui il documento sia carente di uno degli attributi richiesti dalla legge per conseguire valore di piena prova, ma comunque basati sulla presenza di un soggetto certificatore. Un esempio di documento informatico sottoscritto con firma elettronica debole potrebbe essere quello delle *e-mail,* in cui sussiste un collegamento tra un soggetto e il documento attraverso la *password*: naturalmente l'attendibilità di questo documento sarà rimessa al libero apprezzamento del giudice.
4) Documenti informatici privi di qualsiasi firma ed aventi l'efficacia probatoria delle riproduzioni meccaniche. Si tratta di qualsiasi documento informatico, nel significato più lato che questo termine può assumere.

5) LA DATA DEL DOCUMENTO INFORMATICO

La firma digitale, così come la firma autografa, può testimoniare la provenienza di un documento da una determinata persona, ma niente dice a proposito del momento in cui essa è stata posta in essere. L'attribuzione di una data certa ad un documento informatico avviene attraverso una specifica procedura che prende il nome di validazione temporale. La validazione temporale, o *time stamping*, consiste nell'associare al documento informatico una marca temporale che, in modo approssimativo e a-tecnico, potremmo definire come una dichiarazione, proveniente dal certificatore, avente ad oggetto la data e l'ora in cui la marca stessa è stata

apposta. In pratica, chi vuole datare un documento informatico, lo trasmette per via telematica ad un ente abilitato a offrire il servizio di validazione temporale, chiedendo che a quel documento sia apposta la marca temporale. Il certificatore, ricevuta la richiesta, provvede ad associare la marca al documento con lo stesso sistema delle chiavi asimmetriche e poi restituisce al mittente il documento stesso. Le caratteristiche tecniche delle chiavi di marcatura temporale sono disciplinate dall'art 58 delle regole tecniche contenute nel dpcm del 1999. Chiunque può verificare la data utilizzando la chiave pubblica abbinata a quella privata utilizzata dal certificatore per apporre la marca temporale. Il documento informatico potrà così contenere due firme: la sottoscrizione digitale del suo autore e la sottoscrizione digitale del certificatore che ha apposto la marca temporale. La marca temporale è inoltre generata in modo che chi la appone non possa leggere il documento.

Il certificatore, nel rilasciare il certificato, deve determinarne la validità temporale dello stesso. Qualsiasi certificato, sia esso relativo all'apposizione di una firma digitale che all'apposizione di una marca temporale, esaurisce i suoi effetti nell'arco temporale predeterminato dal certificatore. Venendo meno la validità del certificato, viene meno anche l'efficacia probatoria privilegiata del documento informatico e della marca temporale. Per evitare questo inconveniente è possibile, prima della scadenza del certificato, prolungare la validità del documento informatico facendovi apporre una marca temporale. Questa operazione produrrà l'effetto (oltre che di datare il documento), di prorogarne l'efficacia probatoria privilegiata per un periodo pari a quello di scadenza della marca temporale. Naturalmente l'operazione deve essere ripetuta ad ogni singola scadenza. Se non si procede alla rinnovazione

della validazione temporale, quale sarà l'efficacia probatoria del documento informatico il cui certificato sia scaduto di validità? Certamente avrà perso l'efficacia di piena prova fino a querela di falso delle provenienza delle dichiarazioni in esso contenute, ma si può ragionevolmente sostenere che diventi una prova liberamente valutabile dal giudice.

Quindi, mentre la sottoscrizione autografa una volta apposta non necessita di ulteriori attività, oltre a quella della conservazione del supporto cartaceo, viceversa il documento informatico ha un efficacia provvisoria, subordinata alla condizione del verificarso in futuro di determinati eventi.

6) CENNI SULLA RESPONSABILITA' CIVILE DEL CERTIFICATORE E DEL TITOLARE DELLA FIRMA DIGITALE

Prima di analizzare l'argomento è necessario fare una breve premessa sul concetto di falsità materiale in ordine alla firma digitale: per firma digitale falsa si deve intendere quella apposta da un soggetto diverso dal titolare della chiave privata utilizzata. Abbiamo infatti visto in precedenza che con il sistema delle chiavi asimmetriche si riesce a garantire l'integrità del documento, il quale non si presta per sua natura a manomissioni di alcun genere. L'unico modo per costruire un falso materiale è quello di utilizzare una chiave altrui. La sottoscrizione cartacea falsa, infatti, appare materialmente e visivamente diversa da quella autografa, in quanto frutto della grafia di un diverso sottoscrittore. Al contrario, la firma digitale differisce da quella autentica solo per il soggetto che l'ha digitata, ma non è graficamente distinguibile da quella autentica. L'argomento è interessante soprattutto per la conclusione dei contratti via *Internet*, nell'ipotesi in cui chi firma un documento non

sia il legittimo proprietario della chiave: quale rimedio potrà porre in essere l'altro contraente di buona fede che confida nel legittimo utilizzo della firma digitale? Più in particolare, si potrà ritenere comunque valido il contratto e, soprattutto, vincolante nei confronti dell'effettivo titolare della chiave utilizzata abusivamente da altri?

Sussiste una sorta di presunzione che il soggetto che firma un documento sia il titolare effettivo della chiave privata. Non si può tuttavia escludere a priori che qualcuno utilizzi abusivamente la chiave altrui, sottraendola al legittimo proprietario. Il meccanismo di firma digitale, infatti, non consente di identificare il soggetto che materialmente appone la firma, bensì il soggetto titolare della chiave. Si ha notizia di commercialisti che detengono fiduciariamente i dispositivi di firma degli ammini stratori di società loro clienti, per la trasmissione telematica degli atti alle Camere di Commercio, che è obbligatoria a partire dal Dicembre 2002. Si tratta di una grave imprudenza perché è sempre possibile che un malintenzionato si impadronisca di un dispositivo, firmando documenti a nome della società. Per questo motivo il titolare che si sia reso conto che gli è stato sottratto il dispositivo di firma, deve comunicarlo immediatamente al certificatore, che dovrà tempestivamente provvedere alla revoca o alla sospensione del certificato collegato alla chiave privata smarrita o rubata. A partire dal momento della pubblicazione della revoca, chiunque saprà che quella firma digitale non potrà avere nessuna efficacia vincolante nei confronti del legittimo proprietario. Il titolare ha l'obbligo di chiedere immediatamente tali provvedimenti, non appena abbia motivo di ritenere che la chiave non sia più segreta. Inoltre, l'art 9 del dpr n. 513 del 1997 dispone che "*chiunque intenda utilizzare un sistema di chiavi asimmetriche o di firma digitale, è tenuto ad adottare tutte le misure organizzative e*

tecniche idonee ad evitare danno ad altri". Il titolare di una coppia di chiavi, pertanto, risponde dai danni derivanti dalla falsificazione della propria firma se non ha conservato con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne integrità e massima sicurezza, oppure, se non ha immediatamente richiesto al certificatore la revoca o la sospensione in tutti i casi in cui ne abbia perduto il possesso, oppure ancora se la chiave sia difettosa o via sia il sospetto di abusi o falsificazioni da parte di altri

In tutti i casi in cui un contratto sia concluso con un soggetto diverso dal legittimo proprietario della coppia di chiavi, questo non sarà valido e non sarà vincolante nei confronti dell'effettivo titolare della coppia di chiavi, ma quest'ultimo dovrà risarcire i danni all'altro contraente di buona fede che aveva fatto legittimo affidamento sul fatto che la chiave fosse stata utilizzata dal legittimo proprietario. Nel nostro ordinamento, infatti, sussiste il principio in base al quale è possibile che un soggetto possa vincolarne un altro, solo se tra i due soggetti vi sia un valido rapporto di mandato con rappresentanza, in base al quale si agisca in nome e per conto di un altro soggetto: ne è conferma l'inefficacia del contratto concluso dal *falsus procurator*, cioè da colui il quale si spacci rappresentante di un altro soggetto che non può vincolare perché questi non gli ha mai conferito alcuna procura.

Il certificatore, invece, potrà rispondere dei danni derivanti dalla mancata corrispondenza alla realtà di tutti i dati contenuti nei propri certificati, sia che essi ineriscano a dati anagrafici del richiedente, sia che riguardino gli eventuali poteri di rappresentanza e le limitazioni all'uso della coppia di chiavi.

7 BREVE GUIDA ALLE REGOLE TECNICHE.

Come abbiamo già avuto modo di anticipare, il dpr n 513 del 1997 rimandava ad un apposito regolamento la disciplina delle regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. Considerato che tali norme tecniche sono, in realtà, quelle che interessano in maniera più diretta gli operatori tecnici di settore, è opportuno ripercorrere, seppur in sintesi, il loro contenuto.

Tali regole si suddividono in :

1) regole tecniche di base;
2) regole tecniche per la certificazione delle chiavi;
3) regole tecniche sulla validazione temporale e per la protezione dei documenti informatici;
4) regole tecniche per le Pubbliche Amministrazioni e regole finali.

Passiamo, dunque, ad esaminare gli aspetti tecnici essenziali di questo testo normativo.

7.1 IDENTIFICAZIONE DEL TITOLARE

Il punto fondamentale di tutto il meccanismo è quello della identificazione del titolare della coppia di chiavi da parte del certificatore (art 28). Chiunque voglia ottenere la certificazione di una chiave pubblica dovrà formulare una richiesta scritta che deve essere conservata per almeno 10 anni. Ora, non è proprio chiaro come avvenga questa fase di identificazione. Chiaramente occorre un primo contatto tra il richiedente e il certificatore: ciò avverrà attraverso sportelli del certificatore presenti

sul territorio nazionale, oppure attraverso un notaio che abbia stipulato un accordo con il certificatore, oppure ancora individuando dei fiduciari o inviando un incaricato in loco presso Uffici o aziende per il rilascio dei certificati ai dipendenti. Nel 2002, con la comparsa dei primi *kit* per la firma digitale nei negozi di prodotti per ufficio, il riconoscimento è stato affidato a commessi preventivamente identificati ed istruiti in merito. Nel settore bancario la funzione verrà demandata agli addetti agli sportelli.

Dopo l'identificazione, il certificatore fornirà al richiedente un codice segreto per comunicare con lui e, quindi, verrà emesso il certificato: a partire da questo momento il titolare potrà disporre di una coppia di chiavi di cifratura per generare firme digitali.

7.2 Il DISPOSITIVO DI FIRMA

L'art. 1 del dpcm del 1999, lo definisce come un "apparato elettronico programmabile solo all'origine, in grado di conservare in modo protetto la chiave privata e generare al suo interno firme digitali". Si tratta, cioè, di una *smart card* provvista di un microprocessore e di una certa quantità di memoria, al cui interno devono essere presenti la chiave privata del titolare e il software necessario alla generazione delle firme. La caratteristica fondamentale è che deve trattarsi di dispositivo programmabile solo all'origine; in tale dispositivo, cioè, devono essere inserite all'atto della fabbricazione, delle informazioni (identificativo del produttore, numero di matricola, etc), che poi non possono più essere modificate. Questo è il primo e fondamentale dispositivo di sicurezza delle carte a microprocessore, che rende impossibile la loro clonazione: se ogni carta è distribuita con inciso indelebilmente un numero di matricola all'interno, non sarà possibile avere due carte

completamente eguali. Il dispositivo di firma, dunque, non può essere costituito da un floppy disk, perché quest'ultimo non può essere programmato solo all'origine e può essere clonato. Per quanto attiene, invece, alla protezione della chiave, occorre in primo luogo digitare una password per attivarla e, in secondo luogo, che di essa non rimanga traccia all'interno del sistema di validazione usato per apporre la firma. Ecco perché la chiave non deve essere inserita in un PC ma in un dispositivo che, almeno in teoria, il titolare tiene sempre con sé.

7. 3 GENERAZIONE DELLE CHIAVI

Se ne occupa l'articolo 5 del dpcm del 1999 e si tratta di una procedura guidata simile a quella per l'installazione di un software. Occorre assicurare unicità e robustezza della coppia di chiavi, nonché la segretezza della chiave privata. Si tratta di un punto di fondamentale importanza, giacchè, se la procedura di attivazione venisse effettuata da un malintenzionato, tutti i passaggi successivi potrebbero costituire la premessa per qualsiasi operazione illecita. Da un punto di vista strettamente tecnico la robustezza della chiave si ottiene con la lunghezza dell'algoritmo utilizzato: più infatti questo è lungo maggiore sarà il tempo necessario a decifrarlo.

7.4 IL CERTIFICATO

Il certificato costituisce il punto nodale di tutto il sistema. E' un documento informatico, in quanto firmato dal certifcatore, che deve prepararlo e pubblicarlo

rispettando una lunga serie di prescrizioni. Ciascun certificatore deve pubblicare gli indirizzi elettronici attraverso i quali si possa accedere ai registri. Modalità di accesso e formato dei certificati sono disciplinati dagli articoli 11 e 12. Alla firma deve essere allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Nei certificati, inoltre, devono essere inserite altre importantissime informazioni, che consentano a chi riceve il documento una sorta di verifica generale, oltre a quella essenziale dell'integrità dello stesso. Tali requisiti sono tutti disciplinati dall'art 11. E' curioso il fatto che il titolare della coppia di chiavi possa utilizzare uno pseudonimo, del quale però vi deve essere traccia nel certificato.

7.5 REQUISITI DELLE CHIAVI (art 4)

Esistono tre tipi di chiavi: quelle per la firma dei documenti informatici, quelle per la marcatura temporale dei documenti di cui abbiamo già parlato in precedenza e, infine, quelle per la certificazione delle chiavi di sottoscrizione.

7.6 CONERVAZIONE DELLE CHIAVI (ART 8)

Le chiavi vengono conservate e custodite all'interno del dispositivo di firma, che, come abbiamo già detto, consiste in una *smart card*. Il titolare deve conservare questo dispositivo con la massima diligenza possibile e provvedere immediatamente a chiedere la revoca in caso di smarrimento o furto del dispositivo.

7.7 MARCATURA TEMPORALE (ARTT 52 e seguenti)

Si rimanda a quanto precedentemente detto.

7.8 DISPOSIZIONI RELATIVE AI CERTIFICATORI (ARTT 15 e seguenti)

Con il recepimento della normativa europea, non esiste più un unico certifcatore ma si è passati, come abbiamo già visto, ad un sistema di pluralismo.

Precedentemente, per poter diventare certificatore occorrevva un'apposita autorizzazione preventiva dell'A.I.P.A. Oggi, invece, per poter esercitare questa attività non è più necessario ottenere una autorizzazione preventiva,poiché l'attività è stata liberalizzata.

Nella vigente disciplina esistono tre tipi di certificatori:

1) il **certificatore semplice**: in relazione a tutti i tipi di firme elettroniche semplici;
2) **il certificatore qualificato**: ricordiamo che il certificato qualificato è richiesto per la firma digitale e per la firma elettronica qualificata. Per poter essere riconosciuti quali certificatori qualificati occorre dimostrare un alto grado di affidabilità, rispondendo ad una serie di requisiti richiesti dalla legge e occorre preventivamante notificare un avviso all'A.I.P.A, che mantiene comunque un potere di vigilanza e controllo sull'operato dei certificatori, con possibilità di ordinare la cessazione dell'attività laddove il certificatore non dimostri di possedere i requisiti richiesti dalla legge per poter essere riconosciuto come tale;
3) **il certificatore accreditato:** ha un livello di credibilità ancor maggiore rispetto a quello del certificatore qualificato e deve essere inserito in un apposto elenco tenuto e gestito dall'A.I.P.A. Per poter diventare certificatore accreditato occorre costituire una Società per Azioni.

Il certificatore disciplinato dalla normativa italiana dovrebbe divenire automaticamente certificatore accreditato per le garanzie di sicurezza che offre. Infatti, l'accreditamento consiste, come abbiamo già visto, in

un’iscrizione del certificatore in un elenco pubblico consultabile per via telematica e predisposto e aggiornato direttamente dall’A.I.P.A.

La durata del certificato è limitata nel tempo ed è predeterminata dal certificatore stesso al momento del rilascio del certificato. Inoltre, il certificatore che intende cessare la propria attività deve darne preventiva comunicazione all’A.I.P.A, indicando anche il certificatore sostitutivo, in modo da evitare, con la improvvisa uscita dal mercato, l'inutilizzabilità dei documenti sottoscritti con firme i cui certificati non siano più validi poiché non più assistiti da nessun certificatore.