

Raimondo Zagami
rzagami@notariato.it

LA FIRMA DIGITALE

1. IL DOCUMENTO INFORMATICO E LA FIRMA DIGITALE

- 1.1 Firme elettroniche e firma digitale
- 1.2 La cifratura dei dati e la firma digitale
- 1.3 Il dispositivo di firma
- 1.4 Il ruolo delle terze parti fidate
- 1.5 I certificatori
- 1.6 Emissione e pubblicazione dei certificati
- 1.7 La perdita di validità dei certificati

2. IL VALORE GIURIDICO DELLA FIRMA DIGITALE

- 2.1 Il documento informatico
- 2.2 Il documento informatico con firma digitale
- 2.3 Il documento informatico con firma elettronica
- 2.4 Le forme informatiche
- 2.5 L'autenticazione di firma digitale
- 2.6 Le copie informatiche

3. LA VALIDAZIONE TEMPORALE

- 3.1 La validazione temporale
- 3.2 Il documento informatico trasmesso telematicamente
- 3.3 I contratti stipulati con strumenti informatici o per via telematica

Relazioni, rivedute ed aggiornate, scritte per la pubblicazione negli atti del Convegno organizzato da ITA s.r.l. sul tema "La firma digitale", Milano 15-16 novembre 2001.

1 IL DOCUMENTO INFORMATICO E LA FIRMA DIGITALE

1.1 Firme elettroniche e firma digitale

Dal punto di vista giuridico, nell'ordinamento italiano, la "firma digitale" è un tipo di "firma elettronica" che, apposta ad un documento informatico, ne consente l'attribuzione di paternità e la verifica dell'integrità, in modo relativamente sicuro. In conseguenza di ciò, il documento informatico con firma digitale possiede un valore giuridico ed un'efficacia probatoria equiparata a quella propria del documento cartaceo sottoscritto.

Le norme che in Italia disciplinano la firma digitale sono fondamentalmente contenute nel D.P.R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, G.U. n. 42 del 20 febbraio 2001, s.o.) - che ha incorporato le disposizioni del 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'articolo 15, comma 2, della legge 15 marzo 1997, n. 59) - ed in altri provvedimenti tecnici e di dettaglio, tra cui il basilare D.P.C.M. 8 febbraio 1999 (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513). L'art. 78 comma 1 T.U. stabilisce che "Dalla data di entrata in vigore del presente testo unico restano comunque in vigore: [...] f) fino alla loro sostituzione, [...] le regole tecniche già emanate alla data di entrata in vigore del presente testo unico". La deliberazione AIPA 23 novembre 2000, n. 51 reca le Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni; mentre, la circolare AIPA 16 febbraio 2001, n. 27 tratta dell'utilizzo della firma digitale nelle pubbliche amministrazioni.

Dal punto di vista tecnico-informatico, la firma digitale è un insieme di *bit* (dati informatici digitali di base), logicamente associati ad un documento informatico e generati mediante l'utilizzo di un dispositivo di firma, con l'applicazione di complessi algoritmi di cifratura, rispettando precisi requisiti di sicurezza, nel quadro di una cosiddetta infrastruttura di certificazione.

La "firma digitale" rientra, pertanto, nel più ampio *genus* della "firma elettronica", definita e disciplinata dalla direttiva europea del 13 dicembre 1999, n. 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (G.U.C.E. n. L 013 del 19 gennaio 2000), non ancora implementata nell'ordinamento italiano (il termine scadeva il 19 luglio 2001). Ai sensi dell'art. 2 n. 1 della direttiva CE, una firma elettronica (semplice) è costituita da "dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione". Con tale espressione (*electronic signature*) si intende, dunque, qualunque metodo e tecnologia attraverso cui si può firmare un documento informatico. Ad es. la digitalizzazione grafica di una sottoscrizione, la rappresentazione di un dato biometrico, un MAC (*Message Authentication Code*) basato sulla cifratura simmetrica, altri caratteri o dati inseriti dall'autore del documento, la semplice digitazione del nome dell'autore in calce al documento, ecc.

Nel vasto ambito delle firme elettroniche, la direttiva CE definisce, dal punto di vista funzionale, la sottospecie della "firma elettronica avanzata", come "una firma elettronica che soddisfi i seguenti requisiti: a) essere connessa in maniera unica al firmatario; b) essere idonea ad identificare il firmatario; c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati" (art. 2 n. 2 direttiva CE).

Ad es. la rappresentazione grafica digitale di una sottoscrizione (acquisita con *scanner* o tramite tavoletta grafica), oppure la rappresentazione digitale di un dato biometrico (impronta

digitale, della retina, ecc.) apposte in calce ad un documento informatico, pur essendo “firme elettroniche”, ai sensi della direttiva CE, non sono firme elettroniche avanzate. Infatti, tali firme sono connesse in maniera unica al firmatario (requisito *sub. a*), sono idonee ad identificare il firmatario (requisito *sub. b*), ma non sono create con mezzi sul quali il firmatario può conservare il proprio controllo esclusivo (requisito *sub. c*) e non sono collegate ai dati cui si riferiscono in modo da consentirne l’identificazione di ogni modifica (requisito *sub. d*).

La direttiva CE, ai fini degli effetti giuridici delle firme elettroniche (art. 5), distingue, inoltre, la “firma elettronica sicura”, che è tale in quanto creata con un dispositivo di firma che soddisfa specifici requisiti indicati nell’allegato III della direttiva stessa (art. 2 n. 6).

La “firma digitale” disciplinata nell’ordinamento italiano (che non utilizza la locuzione “firma elettronica”), basata sulla specifica tecnologia della cifratura dei dati, è una specie del genere più ampio della “firma elettronica avanzata” di matrice comunitaria, la quale a sua volta è una specie del genere “firma elettronica”. In altri termini, è concepibile una “firma elettronica avanzata” diversa dalla “firma digitale”, anche se allo stato dell’attuale tecnologia non si conoscono tecnologie altrettanto efficaci agli stessi fini, che soddisfano tutti i requisiti prescritti dall’art. 2 n. 2 della direttiva CE. Peraltro, la direttiva CE, che non utilizza mai l’espressione “firma digitale”, e lascia il campo a diverse tecnologie, in ossequio ai principi del mercato e della neutralità tecnologica, è stata evidentemente scritta pensando alla specifica tecnologia della firma digitale.

1.2 La cifratura dei dati e la firma digitale

La firma digitale è basata sulla tecnologia della cifratura asimmetrica (o a chiave pubblica) dei dati informatici.

Cifrare (*encipher* o *encode*) significa trasformare i dati in una forma incomprensibile ed illeggibile da parte di chi non possieda la chiave per effettuare l’operazione inversa di decifratura (*decipher* o *decode*). La cifratura si realizza mediante l’applicazione di un algoritmo di cifratura (*cipher system*) e di una chiave; la funzione è reversibile, per cui la decifratura si compie mediante l’applicazione dello stesso algoritmo e della chiave ai dati cifrati (criptogramma o *ciphertext*) e restituisce il dato originale (testo in chiaro o *plaintext*).

Si distinguono sistemi di cifratura in relazione allo scopo cui sono diretti ed al modo di impiego delle chiavi. Ad una cifratura a scopo di segretezza, volta a rendere i dati non conoscibili; si contrappone una cifratura a scopo di autenticazione, volta al raggiungimento dei risultati della verifica della provenienza e dell’integrità dei dati. Per il raggiungimento di entrambi gli scopi (segretezza ed autenticazione, congiuntamente o alternativamente) sono utilizzabili sia sistemi di cifratura detti simmetrici, che sistemi di cifratura detti asimmetrici.

Il T.U., in quanto provvedimento incorporante il D.P.R. n. 513/1997 che riguardava solo l’autenticazione dei documenti, pur prevedendo la cifratura a scopo di segretezza (art. 22 comma 1 lett. b-c-d T.U.), non ne contiene alcuna disciplina, rinviando ad emanande regole tecniche le misure volte a garantire la riservatezza (confidenzialità) delle informazioni contenute nel documento informatico (art. 8 comma 3 T.U.). La cifratura a scopo di segretezza pone, poi, problemi giuridici e politici del tutto peculiari, collegati ai diritti dei cittadini a scambiare comunicazioni riservate difficilmente decrittabili anche da parte delle forze di polizia.

Un sistema di cifratura è detto simmetrico (o a chiave singola, o a chiave privata, o a chiave segreta) quando la stessa ed identica chiave è usata sia per cifrare che per decifrare i dati.

I sistemi simmetrici presentano notevoli inconvenienti, derivanti dai problemi di moltiplicazione, scambio e gestione delle chiavi, che ne rendono difficile l’uso negli ambiti di reti aperte tipo Internet, e dalla mancanza di possesso esclusivo della chiave di cifratura, che

non consente l'apposizione di firme elettroniche avanzate (requisito *sub. c* dell'art. 2 n. 2 direttiva CE), ma solo di semplici firme elettroniche non avanzate come un MAC (*Message Authentication Code*).

I sistemi di cifratura asimmetrica, ideati nel 1976, superano i limiti dei sistemi simmetrici. Un sistema di cifratura asimmetrico (o a chiave pubblica) funziona con coppie di chiavi tra loro diverse e matematicamente collegate, formate da una chiave privata e da una chiave pubblica: ciò che una chiave cifra, solo l'altra decifra. La chiave privata è strettamente personale e deve essere custodita segretamente, mentre la chiave pubblica è destinata ad essere divulgata. È essenziale per la sicurezza del sistema che la chiave privata non sia ricavabile dalla corrispondente chiave pubblica. La funzione matematica e più in generale il metodo di cifratura è definito algoritmo. Le regole tecniche prescrivono che "Per la generazione e la verifica delle firme digitali possono essere utilizzati i seguenti algoritmi: a) RSA (Rivest-Shamir-Adleman algorithm); b) DSA (Digital Signature Algorithm)" (art. 2 reg. tec.).

Il T.U. definisce, con una descrizione idonea a ricomprendere sia l'utilizzo delle chiavi a scopo di segretezza che quello a scopo di autenticazione, come "chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici" (art. 22 lett. b T.U.); viene definita "chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica" (art. 22 lett. c T.U.); viene definita "chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, 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" (art. 22 lett. d T.U.).

La cifratura asimmetrica può essere utilizzata, in primo luogo, a scopo di segretezza. Il messaggio da segretare viene cifrato con la chiave pubblica del destinatario; quindi, viene decifrato da quest'ultimo con la corrispondente chiave privata della coppia. Tuttavia, si preferisce non utilizzare, a tale scopo direttamente ed esclusivamente i cifrari asimmetrici, ma una combinazione di entrambi i sistemi simmetrico ed asimmetrico (*hybrid cryptosystem* o *dual encryption approach*). Il testo in chiaro è cifrato con un cifrario simmetrico, la cui chiave (*session key*, preferibilmente casuale) è inviata in forma cifrata con un sistema asimmetrico applicando la chiave pubblica del destinatario. Questo perché la cifratura asimmetrica richiede calcoli molto più complessi di quella simmetrica e, pertanto, è molto più lenta a parità di dati da cifrare. I cifrari asimmetrici, a parità di lunghezza delle chiavi, sono, poi, molto meno sicuri dei cifrari simmetrici. Inoltre, la corretta cifratura mediante sistemi asimmetrici presuppone dati di lunghezza non superiore alla chiave utilizzata.

Per l'apposizione di firme digitali (controllo di integrità e provenienza) con un sistema di cifratura asimmetrico, rispetto alla cifratura a scopo di segretezza, si inverte l'uso delle chiavi, fermo restando l'algoritmo utilizzato. La chiave privata del mittente si utilizza per firmare il documento; la corrispondente chiave pubblica (dello stesso firmatario) si impiega per verificarne l'autenticità.

In relazione al modo di generazione, all'uso cui sono destinate ed al tipo di certificazione di cui sono oggetto, le regole tecniche distinguono diverse tipologie di chiavi: "a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti; b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati ed alle loro liste di revoca (CRL) o sospensione (CSL); c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali" (art. 4 comma 4 reg. tec.). "Non è consentito l'uso di una chiave per funzioni diverse da quelle

previste dalla sua tipologia” (art. 4 comma 5 reg. tec.). La tipologia della chiavi deve potersi desumere in modo inequivocabile dal certificato (art. 11 comma 2 reg. tec.).

La cifratura asimmetrica si svolge correttamente solo su dati di lunghezza non superiore alla chiave ed, inoltre, richiede notevoli capacità di calcolo (essendo molto più lenta di quella simmetrica). Pertanto, per ragioni di maggiore sicurezza e di velocità nell’elaborazione, si preferisce applicare la chiave privata non sull’intero messaggio, bensì solo sulla sua impronta digitale (detta anche *hash code*, *message digest*, *digital fingerprint*). L’impronta è una sorta di sintesi matematica del messaggio, calcolata applicando una funzione di *hash* (detta anche *message digest algorithm* o funzione di contrazione), che restituisce una stringa di dimensioni fisse, di lunghezza inferiore alla chiave di cifratura.

Le funzioni di *hash* da impiegare devono essere:

- a) pubbliche, quindi chiunque può ripetere il calcolo se possiede il documento originale;
- b) *one-way function*, non è possibile ricostruire il documento dalla sua impronta, cioè trovare un certo *input* che produce quella data impronta;
- c) a risultato fisso, cioè produrre sempre la stessa impronta e di dimensione fissa in relazione allo stesso documento;
- d) *collision free*, cioè non è impossibile che due documenti diversi producano la stessa impronta, ma è altamente improbabile, computazionalmente impraticabile. In altri termini, il messaggio non può essere sostituito senza modificare anche la relativa impronta. Tale requisito non va inteso in senso assoluto, poiché le collisioni sono inevitabili, dato che l’insieme delle possibili impronte è molto minore dell’insieme dei possibili documenti. Senonché, la maggior parte delle collisioni si riferirà a documenti inutilizzabili (non aventi un significato) per l’eventuale falsificatore.

Le regole tecniche definiscono per “funzione di hash”, una “funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali” (art. 1 lett. c reg. tec.); per “impronta” di una sequenza di simboli binari, la “sequenza di simboli binari di lunghezza predefinita generata mediante l’applicazione alla prima di una opportuna funzione di hash” (art. 1 lett. b reg. tec.).

L’apposizione di una firma digitale consiste in un’operazione matematica di cifratura dell’impronta di un documento informatico, mediante una chiave privata ed un cifrario asimmetrico. La verifica di una firma digitale consiste nell’operazione inversa di decifratura, mediante l’applicazione della corrispondente chiave pubblica. Supponendo che Tizio voglia firmare un documento da spedire a Caio per posta elettronica, l’apposizione di una firma digitale, con il calcolo dell’impronta, richiede le seguenti operazioni:

- 1) calcolo dell’impronta I da parte di Tizio, applicando la funzione pubblica di *hash* al messaggio M;
- 2) calcolo della firma digitale F sull’impronta I applicando la chiave privata K_S di Tizio con un algoritmo asimmetrico;
- 3) spedizione del messaggio in chiaro M (o segretato) e della firma digitale F, insieme o separatamente;
- 4) applicazione della funzione di *hash* al messaggio in chiaro M, ed ottenimento dell’impronta I, da parte di Caio;
- 5) decifrazione, sempre da parte di Caio, della firma digitale F mediante applicazione della chiave pubblica K_P di Tizio;
- 6) confronto tra l’impronta ottenuta al punto 4) e l’impronta ottenuta al punto 5): se risultano identiche, la firma è verificata positivamente.

Un eventuale impostore Sempronio difficilmente potrebbe inviare falsamente un messaggio a nome di Tizio, in quanto, pur potendo generare la medesima impronta (le funzioni di *hash* sono pubbliche), non potrebbe poi cifrarla dato che si presume non conosca la chiave privata di Tizio.

Nemmeno potrebbe copiare la firma digitale di Tizio ed applicarla ad un altro messaggio, in quanto, così facendo, il nuovo messaggio produrrebbe un'impronta non corrispondente a quella derivante dalla decifrazione della firma digitale.

Infine, qualunque alterazione (anche di un solo *bit*) del documento firmato, sarebbe immediatamente rilevabile dalla non corrispondenza tra l'impronta derivante dalla decifrazione della firma digitale e quella ricalcolata dal destinatario Caio sul messaggio in chiaro.

La firma digitale calcolata sull'impronta consiste in una, più o meno breve, stringa di caratteri alfanumerici che è (normalmente) unita quale appendice al messaggio ed archiviata e trasmessa con esso. Tuttavia, può anche essere mantenuta in un *file* distinto, conservata e trasmessa separatamente, purché sia ricollegabile al messaggio cui si riferisce, senza pregiudicare la possibilità di una sua corretta verifica dell'autenticità, e senza possibilità che la firma (pur facilmente duplicabile) sia riutilizzata per altri e diversi documenti. Secondo il T.U. "a ciascun documento informatico [...] può essere apposta o associata con separata evidenza informatica, una firma digitale" (art. 23 comma 1 T.U.).

Il T.U. definisce la "firma digitale" in relazione alla sua essenza tecnica ed al suo scopo, quale "risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore tramite la chiave privata ed 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" (art. 1 lett. b T.U.). Ribadendo la funzione di controllo di provenienza ed integrità, è ulteriormente prescritto che "La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata" (art. 23 comma 3 T.U.).

L'applicazione di una firma digitale non fornisce di per sé anche la segretezza del messaggio. Per ottenere questo risultato dovrà essere cifrato anche il testo in chiaro (prima o dopo l'apposizione della firma digitale) applicando la chiave pubblica asimmetrica del destinatario, oppure seguendo il suddetto schema del *dual encryption*. Quando si spedisce un messaggio nello stesso tempo segretato e firmato, si parla di *digital envelope*, in quanto si realizzerebbe un'analogia di risultati con l'invio di una lettera sottoscritta ed inserita in una busta chiusa. Alcuni algoritmi di cifratura a chiave pubblica (ad es. RSA) sono utilizzabili indifferentemente per segretare e per generare firme digitali (invertendo l'uso delle chiavi); mentre, altri algoritmi sono specificamente ideati per l'apposizione e la verifica di firme digitali (ad es. DSA) e non consentono la segretazione del messaggio mediante l'inversione dell'uso delle chiavi.

1.3 Il dispositivo di firma

Le operazioni per la generazione e per la verifica delle firme digitali sono eseguite in modo automatico e trasparente per l'utente, da appositi *software* di semplice utilizzo. Il comportamento richiesto all'utente per l'apposizione di una firma digitale è completamente diverso dall'apposizione di una sottoscrizione cartacea, mancando una tangibile e visibile relazione tra documento e firma. Per garantire il sottoscrittore sull'esattezza del documento firmato, è stabilito che "Gli strumenti e le procedure utilizzate per la generazione, l'apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, chiaramente e senza ambiguità, i dati a cui la firma si riferisce e richiedere conferma della volontà di generare la firma" (art. 10 comma 1 reg. tec.).

In pratica, si utilizzerà un normale *computer* dotato dell'*hardware* per l'interfacciamento con il dispositivo di firma (ad es. lettore *smart card*) e del *software* necessario per la gestione delle firme: con l'apposito programma si seleziona il documento da firmare (ad es. un *file* prodotto da un elaboratore testi in un formato standard), che deve essere presentato chiaramente e senza ambiguità; si dà "conferma della volontà di generare la firma" (ad es. cliccando con il *mouse* un apposito pulsante sullo schermo); si inserisce il dispositivo di firma (ad es. una *smart card*) dove è contenuta la chiave privata; si abilita il dispositivo di firma (ad es. inserendo una *password* o esibendo una parte del corpo per il riconoscimento biometrico), il quale procederà al suo interno al calcolo della firma digitale, che verrà associata al documento.

Per converso, la verifica di una firma digitale si compie utilizzando un normale *computer* senza particolare *hardware* aggiuntivo (non occorre una *smart card*), sul quale gira un apposito programma: selezionato il documento, il programma verifica la firma in relazione al suo certificato (controllandone la persistente validità *on-line* in tempo reale). Ugualmente, è prescritto che "Gli strumenti e le procedure utilizzate per [...] la verifica delle firme digitali debbono presentare al sottoscrittore [ed anche al verificatore], chiaramente e senza ambiguità, i dati a cui la firma si riferisce" (art. 10 comma 1 reg. tec.).

Il "dispositivo di firma" è definito come "un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali" (art. 1 lett. d reg. tec.). Nel caso in cui il titolare voglia effettuare autonomamente la generazione della coppia di chiavi di cifratura, il dispositivo di firma deve avere anche la capacità di eseguire tale operazione al suo interno (art. 6 comma 3 reg. tec.). Può funzionare da dispositivo di firma la carta di identità elettronica rilasciata su supporto informatico, prevista dall'art. 2 comma 10, legge n. 127/1997 (come modificato dall'art. 2 comma, 4 legge n. 191/1998) e disciplinata dal D.P.C.M. 22 ottobre 1999, n. 437 (in particolare l'art. 4).

La prima funzione del dispositivo di firma è quella di conservare le chiavi private, dati informatici relativamente lunghi (anche oltre 4000 *bit*), formati da sequenze di caratteri senza senso compiuto, impossibili da ricordare a mente. Nelle regole tecniche si legge che "Le chiavi private sono conservate e custodite all'interno di un dispositivo di firma. È possibile utilizzare lo stesso dispositivo per conservare più chiavi. [...] Per fini particolari di sicurezza, è consentita la suddivisione della chiave privata su più dispositivi di firma" (art. 8 commi 1 e 3 reg. tec.).

Il dispositivo di firma, per ragioni di sicurezza, deve avere anche la capacità di elaborazione per il calcolo della firma digitale al suo interno (art. 10 comma 3 reg. tec.). "La generazione della firma deve avvenire all'interno di un dispositivo di firma così che non sia possibile l'intercettazione del valore della chiave privata utilizzata" (art. 10 comma 3 reg. tec.). In tal modo, si esclude qualunque trasmissione della chiave privata al suo esterno, evitando così rischi di intercettazione ed uso fraudolento. Qualunque tentativo di manomissione della *smart card* o del dispositivo di firma in generale dovrebbe portare all'autodistruzione del suo contenuto.

In un sistema di autenticazione basato sulla cifratura asimmetrica, la presunzione di provenienza della firma e dei documenti informatici deriva dal possesso e disponibilità esclusivi della chiave privata. Il dispositivo di firma è, quindi, uno strumento di uso strettamente personale, il quale non può essere assolutamente consegnato ed utilizzato da altri in tutti i casi in cui non sia ammessa la delega della firma (tipicamente per le funzioni notarili). È prescritto che "Il titolare delle chiavi deve: a) conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza; b) conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; c. richiedere immediatamente la revoca delle

certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi” (art. 8 comma 4 reg. tec.).

Per limitare l’abuso del dispositivo di firma, è stabilito che, “prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all’identificazione del titolare” (art. 10 comma 4 reg. tec.).

A tal fine, il T.U. prevede l’impiego delle tecnologie di riconoscimento biometrico (ad es. impronte digitali, della mano, della retina, timbro della voce, dna, ecc.), definendo “chiave biometrica, la sequenza di codici informatici utilizzati nell’ambito di meccanismi di sicurezza che impiegano metodi di verifica dell’identità personale basati su specifiche caratteristiche fisiche dell’utente” (art. 22 lett. e T.U.). Si rinvia, poi, alle regole tecniche per “dettare le misure tecniche, organizzative e gestionali volte a garantire l’integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all’eventuale uso di chiavi biometriche” (art. 8 comma 3 T.U.).

Tuttavia, le regole tecniche emanate non contengono ancora espliciti riferimenti all’impiego di tecniche di riconoscimento biometriche per l’identificazione del titolare della chiave privata. Nell’art. 8 comma 4 lett. b reg. tec. si parla piuttosto di “informazioni di abilitazione all’uso della chiave privata”, che vanno conservate in luogo diverso dal dispositivo contenente la chiave stessa (ad es. PIN o *password*).

Pertanto, in attesa dell’emanazione di standard consolidati, allo stato attuale non è vi è alcuna prescrizione obbligatoria riguardo l’uso dei sistemi biometrici, che rimangono di adozione facoltativa e, comunque, quantomai opportuni in ambiti in cui sono richieste garanzie di sicurezza aggiuntive rispetto a quelle ordinariamente presenti. Ad es. per le chiavi private dei notai, il sistema di riconoscimento biometrico consentirebbe di realizzare nel massimo grado il legame personale tra chiave e soggetto titolare, garantendo la provenienza della firma dallo stesso notaio ed escludendo ragionevolmente ogni eventuale dubbio circa possibili deleghe nell’uso della carta e nella firma.

Non è precisato esattamente nelle regole tecniche in cosa dovrà consistere il dispositivo di firma, il quale nella prima fase, per gli utenti, sarà rappresentato da una carta elettronica a microprocessore (*smart card, chip card, crypto card*), o altro strumento (ad es. *token USB*), di caratteristiche standard, che contiene al suo interno una memoria digitale ed un microprocessore che comunicano all’esterno per mezzo di contatti elettrici posti nella superficie esterna della carta, funzionanti con un mini sistema operativo in grado di far girare applicazioni per il compimento delle operazioni di cifratura. Nel manuale operativo del certificatore (art. 45 reg. tec.), tra le altre clausole contrattuali, saranno indicate le esatte caratteristiche tecniche dei dispositivi di firma.

In ogni caso, i requisiti prescritti dalle regole tecniche italiane, rendono il dispositivo di firma conforme al “dispositivo per la creazione di una firma sicura” previsto dalla direttiva comunitaria (art. 2 n. 6 e allegato III direttiva CE).

1.4 Il ruolo delle terze parti fidate

La firma digitale, come fin qui delineata, a seguito della verifica tecnica, offre soltanto due (relative) certezze: in primo luogo, che la firma stessa è stata generata impiegando la chiave privata corrispondente a quella pubblica utilizzata per la verifica; in secondo luogo, che il documento informatico firmato non è stato modificato dal momento della generazione della firma stessa (integrità). Scrivo *relative* certezze, perché non è mai teoricamente impossibile falsificare una firma, bensì solo estremamente difficile, richiedendosi straordinarie capacità di calcolo e lunghissimi tempi di elaborazione, con ingenti investimenti, direttamente proporzionali al livello di sicurezza adottato.

Di per sé, la verifica tecnica di una firma digitale non è in grado di offrire alcuna risultanza probatoria riguardo all’identità del soggetto sottoscrittore (la provenienza del

documento). La correlazione tra chiave pubblica e chiave privata è, infatti, soltanto di tipo matematico. Diversamente, una sottoscrizione cartacea, eventualmente a seguito di verifica, consente di stabilire un collegamento immediato e diretto tra sottoscrizione stessa e soggetto sottoscrittore.

La sottoscrizione cartacea è, infatti, un dato somatico e personale, che risulta in un segno diverso per ogni soggetto che l'appone. La firma digitale, invece, risulta dall'applicazione di un dato informatico (la chiave privata), un mezzo tecnico, astrattamente (anche se in certi casi illecitamente) utilizzabile da chiunque, in modo del tutto analogo ad un sigillo. Pertanto, firme digitali apposte da soggetti diversi sullo stesso documento, ma utilizzando la stessa chiave e lo stesso algoritmo, non sono tra loro tecnicamente distinguibili in sede di verifica.

Peraltro, mentre appare delegabile l'uso del sigillo, in quanto si affianca normalmente ad una sottoscrizione autografa, invece, deve essere fortemente ribadito che non è delegabile l'uso del dispositivo di firma quando non è delegabile la relativa facoltà di firmare (ad es. per i notai nell'esercizio delle loro funzioni). In altri termini, da una parte, la chiave privata è analoga quanto a struttura ed a modalità applicative all'uso di un sigillo, mentre, da un'altra parte, è analoga quanto a risultati ed a responsabilità all'apposizione di una sottoscrizione autografa.

Si è detto prima come possa limitarsi l'uso della chiave privata al suo titolare (possesso della carta, PIN e *password*, biometria). Si tratta ora di stabilire un legame tra la firma digitale apposta ed il soggetto firmatario, tra il documento informatico ed il suo autore, in modo che in sede di verifica della firma si possa riconoscerne l'autore (o presunto tale). Per ottenere questo importante risultato, sembra che non si possa prescindere dall'intervento di una terza parte fidata ed imparziale.

A) In primo luogo, il legame tra la coppia di chiavi ed un'identità soggettiva può essere posto mediante l'intervento della terza parte fidata che certifica la titolarità della coppia di chiavi in capo ad un determinato soggetto previamente identificato (art. 28 comma 2 lett. a T.U.).

Il T.U. definisce per "certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato" (art. 22 comma 1 lett. f T.U.).

La verifica di una firma digitale cui corrisponde una chiave pubblica certificata consente di ottenere un'identità soggettiva cui ricollegare la chiave stessa e, dunque, la firma. Il T.U., sul piano probatorio, ricollega a tale tipo di certificazione, l'efficacia di scrittura privata *ex art.* 2702 c.c.

Però, si badi bene, con la sola certificazione della chiave, non si ha la certezza che Tizio, titolare della chiave come risulta dal certificato, ha apposto la firma utilizzando la correlata chiave privata; bensì, soltanto che la firma stessa è stata apposta utilizzando la chiave privata di titolarità di Tizio. Tecnicamente, non si può conoscere l'autore della firma, ma solo il soggetto titolare della chiave. Resta incerto se la chiave privata sia stata utilizzata realmente da Tizio nell'apporre la firma o se, invece, non sia stata utilizzata concretamente da Caio.

Si ribadisce, infatti, che la chiave privata è un dato informatico, uno strumento tecnico, contenuto in una *smart card*, utilizzabile astrattamente da chiunque. Una firma digitale, non essendo un dato somatico, è sempre uguale (se apposta con la stessa chiave e sullo stesso documento) e, quindi, correttamente (matematicamente) verificabile, anche se apposta da soggetti diversi. Così, nello scambio di dichiarazioni telematiche tra persone distanti, il destinatario - oppure chi verifica un documento *ex post* - non può avere la certezza che la

firma digitale che riceve, ancorché verificata con un certificato valido (non scaduto e non revocato o sospeso), sia stata effettivamente apposta dal titolare della chiave.

Per limitare l'uso della chiave privata al legittimo titolare, come si è detto, le regole tecniche stabiliscono che "il dispositivo di firma deve procedere all'identificazione del titolare" (art. 10 comma 4 reg. tec.), limitandone così l'uso da parte di una persona diversa. I primi dispositivi di firma sono delle *smart card* protette da un codice segreto come un PIN o una *password*. Tuttavia, questo codice non è inattaccabile; inoltre, è concepibile una cessione volontaria della chiave ad altri (unitamente al codice di abilitazione), oppure una sua decifrazione fraudolenta mediante attacco al cifrario.

Anche l'eventuale impiego dei dati biometrici quale strumento per l'accesso alla chiave privata, pur aumentando notevolmente il grado di sicurezza nella "esclusività" della chiave, non renderebbe, comunque, "personale" o "somatica" la firma digitale, nel senso di come tale requisito si intende per la sottoscrizione.

I dati biometrici, come anche i PIN e le *password*, hanno la stessa funzione di strumento di controllo per l'accesso ai sistemi informatici (*simple authentication* secondo la raccomandazione ITU X.509), nel caso specifico per limitare l'uso del mezzo tecnico (cioè la chiave). Si contrappongono alla firma digitale che consente di creare documenti di cui sia possibile verificare *ex post* l'integrità e provenienza (*strong authentication* secondo la raccomandazione ITU X.509). Di per sé utilizzato, il dato biometrico non consentirebbe di stabilire alcun legame tra un soggetto ed un documento, dato che non dipende dal contenuto del documento, ed è riutilizzabile.

B) Occorre, quindi, risolvere questo secondo problema del legame tra la firma digitale concretamente apposta e l'identità soggettiva del reale firmatario.

Ancora una volta si richiede l'intervento certificadorio di una terza parte fidata, la quale, essenzialmente, assiste di persona alla concreta apposizione (generazione) della firma sul documento informatico e ne certifica il fatto, previa identificazione soggettiva del firmatario, con l'emissione di apposita certificazione a sua volta firmata digitalmente. In tal modo, la verifica di un certificato di tale tipo, se fidato, esclude la circostanza che la firma digitale sia stata apposta da persona diversa dal titolare della relativa chiave.

Questo tipo di certificato è definito dalle *Digital Signature Guidelines dell'American Bar Association* (1996) e dal *Digital Signature Act* dello Utah (1995-1996), come *Transactional certificate* (o anche *attesting certificate*, o *notarial certificate*) per contrapporlo ai certificati prima esaminati (che, invece, collegano la chiave pubblica al soggetto), definiti come *Identifying certificates* (certificati di identità).

Rispetto ai certificati d'identità, i certificati di attestazione devono essere emessi dopo la relativa firma digitale, hanno un contenuto diverso e, per loro natura, sono certificati riferibili ad un singolo atto (mentre un *identity certificate* si riferisce ad un numero indefinito di futuri atti); non hanno un *operational period*, cioè non hanno inizio, né fine di validità; non rileva neanche la revoca o sospensione, dato che si basano su una singola (o più transazioni) e non su un periodo di tempo di validità.

La normativa italiana sulla firma digitale accoglie sostanzialmente la figura del *Transactional certificate* e la inquadra nell'ordinamento vigente configurandola come un'autenticazione di firma (art. 24 T.U.), ed assegnandone la responsabilità primariamente al notaio, quale terza parte fidata ed imparziale. Sul piano probatorio, il T.U. attribuisce a tale tipo di certificazione l'efficacia della scrittura privata autenticata *ex art. 2703 c.c.*

1.5 I certicatori

Il "certificatore" (*Certification Authority*) è definito dal T.U., come "il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima" (art. 22 comma 1 lett. i T.U.).

Il certificato (*Digital ID*) è un documento informatico che essenzialmente associa una chiave pubblica ad un'identità personale. Il certificato è emesso preliminarmente ed è poi valido per verificare una moltitudine successiva ed indeterminata di firme digitali, salvo una sua cessazione di validità (per scadenza, sospensione o revoca). L'autenticità dei certificati, cioè la loro provenienza dal certificatore e l'integrità del loro contenuto, è garantita dalla firma digitale apposta dall'emittente. I dati contenuti nel certificato sono efficaci ed opponibili nei confronti del suo titolare (art. 22 comma 1 lett. n T.U.). Per consentire l'interoperabilità, cioè il reciproco riconoscimento, tra i certificati emessi da diversi certificatori si sono adottati dei formati comuni, codificati nella circolare AIPA 19 giugno 2000, n. 24, recante le Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

La certificazione delle chiavi pubbliche si inserisce nel più vasto contesto di una cosiddetta infrastruttura a chiave pubblica (*Public Key Infrastructure*, PKI), intesa come complesso di procedure, standard, sistemi, norme, regole che governano l'uso dei certificati e delle chiavi pubbliche e private in un sistema di autenticazione per firme digitali.

Le due operazioni basilari comuni a tutte le PKI sono la certificazione (come sopra precisata) e la validazione, cioè il processo di verifica della persistente validità dei certificati già emessi. Entrambe si basano sull'imprescindibile intervento di terze parti fidate. Il modo in cui sono implementate queste due funzionalità base, caratterizza e distingue i diversi possibili modelli di PKI, in relazione diverse variabili.

La direttiva comunitaria, in aderenza al principio di "accesso al mercato", stabilisce che, "al fine di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte" (considerando n. 10 direttiva CE), "gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione" (art. 3 comma 1 direttiva CE; considerando n. 21, secondo cui "il riconoscimento giuridico delle firme elettroniche dovrebbe basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione").

Tuttavia, "gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi volti a fornire servizi di certificazione di livello più elevato" (art. 3 comma 2 direttiva CE), a cui i prestatori di servizi di certificazione dovrebbero essere liberi di aderire e di trarne vantaggio (considerando n. 11 direttiva CE); "gli Stati membri non dovrebbero vietare ai prestatori di servizi di certificazione di operare al di fuori dei sistemi di accreditamento facoltativo" (considerando n. 12 direttiva CE). Tuttavia, secondo l'art. 3 comma 7 direttiva CE, "Gli Stati membri possono assoggettare l'uso delle firme elettroniche nel settore pubblico ad eventuali requisiti supplementari". Questa scriminante è ad es. applicabile per le firme elettroniche da impiegare da parte dei notai italiani nell'esercizio delle loro funzioni e per le firme elettroniche nel cosiddetto processo telematico (D.P.R. n. 123/2001).

La direttiva CE, parallelamente alla distinzione tra firme elettroniche semplici ed avanzate, distingue poi tra "certificato" (semplice), "un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona" (art. 2 n. 9 direttiva CE) e "certificato qualificato", un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II" (art. 2 n. 10 direttiva CE). Peraltro, è importante rilevare che l'emissione di certificati qualificati non è riservata ai soli certificatori accreditati. Indipendentemente da eventuali sistemi di accreditamento facoltativi, la direttiva CE stabilisce, inoltre, che "Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilasci al pubblico certificati qualificati" (art. 3 comma 3 direttiva CE).

Sotto questo profilo, l'attuale normativa italiana richiederebbe alcuni aggiustamenti per adeguarsi pienamente alle prescrizioni della direttiva comunitaria. Peraltro, già oggi prima dell'attuazione della direttiva, nell'ordinamento italiano non è proibita la prestazione di servizi di certificazione operanti al di fuori della disciplina dettata dal T.U. Le norme del T.U., delle regole tecniche e degli altri provvedimenti collegati disciplinano solo l'infrastruttura di certificazione minima da implementare per l'apposizione e la verifica di firme digitali (firme elettroniche avanzate) equivalenti alla sottoscrizione.

Secondo la vigente disciplina, non ancora modificata dall'attuazione della direttiva CE, per esercitare l'attività di certificazione, con gli effetti giuridici di cui al T.U., occorre che il certificatore sia incluso in un apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto ed aggiornato dall'Autorità per l'Informatica nella Pubblica Amministrazione (art. 27 T.U.) e da quest'ultima sottoscritto digitalmente (art. 15 comma 2 reg. tec.). L'inclusione nell'elenco pubblico consegue all'accettazione da parte dell'AIPA di un'apposita richiesta di iscrizione presentata dal certificatore (art. 16 reg. tec.), che deve possedere specifici requisiti indicati dal T.U. (art. 27 comma 3 T.U.). Il contenuto e le modalità di presentazione della domanda sono disciplinati dall'art. 16 commi 2 e 3 reg. tec. e, più dettagliatamente, dalla circolare AIPA 26 luglio 1999, n. 22, emessa sulla base della delega contenuta nello stesso art. 16 comma 1 reg. tec. Il certificatore deve predisporre un manuale operativo (*certification practice statement*) che "definisce le procedure applicate dal certificatore nello svolgimento della propria attività" (art. 45 comma 1 reg. tec.).

La circolare AIPA 13 luglio 2000, n. 26, individua 8 società iscritte nell'elenco pubblico dei certificatori alla data del 6 luglio 2000. Attualmente i certificatori iscritti sono 13, compreso il Centro Tecnico per l'assistenza ai soggetti che utilizzano la rete unitaria della pubblica amministrazione, il quale "è iscritto nell'elenco pubblico dei certificatori con riferimento ai compiti definiti dal decreto del Presidente della Repubblica 23 dicembre 1997, n. 522 ed è tenuto all'osservanza delle disposizioni delle presenti regole tecniche" (art. 16 comma 5 reg. tec.).

1.6 Emissione e pubblicazione dei certificati

Le regole tecniche distinguono tra registrazione e certificazione (in senso stretto), attribuendone entrambi i compiti allo stesso soggetto certificatore. La registrazione, che verrà eseguita presso uffici periferici del certificatore localizzati nel territorio (ad es. sportelli bancari, punti vendita, ecc.), è volta fundamentalmente all'accertamento dell'identità personale del richiedente la certificazione (art. 22 reg. tec.); la certificazione, gestita a livello centralizzato, è volta all'emissione e gestione dei certificati (art. 27 reg. tec.). Mentre la richiesta di registrazione può essere fatta una sola volta presso lo stesso certificatore; la certificazione può essere richiesta più volte sulla base dell'unica precedente registrazione.

Prima di ottenere la certificazione della chiave, il titolare deve procedere ad una registrazione presso il certificatore (art. 22 comma 1 reg. tec.). "La richiesta di registrazione deve essere redatta per iscritto e deve essere conservata dal certificatore per almeno 10 anni" (art. 22 comma 1 reg. tec.).

Con la richiesta di registrazione, accettata dal certificatore, si stipula un contratto di certificazione tra titolare della chiave e certificatore, che concorre a definire i rispettivi obblighi e diritti, in aggiunta ed a specificazione delle norme di legge, con l'adesione da parte dell'utente al manuale operativo predisposto dal certificatore stesso (art. 45 reg. tec.).

"Al momento della registrazione il certificatore deve verificare l'identità del richiedente" (art. 22 comma 2 reg. tec.). Dato che la funzione essenziale del certificatore è fornire garanzia "della corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene" (art. 22 lett. f T.U.), il suo primo obbligo, connotato a questa stessa funzione, è quello di "identificare con certezza la persona che fa richiesta della certificazione" (art. 28 comma 2

lett. a T.U.). Le modalità per l'identificazione non sono prestabilite, ma è lasciata al certificatore la facoltà di definirle, pubblicandole nel proprio manuale operativo (art. 22 comma 3 reg. tec.).

Quello dell'identificazione è un momento molto delicato, fondamento del valore giuridico e dell'efficacia probatoria (presuntiva) del meccanismo della firma digitale. L'adozione di procedure che non consentano un'identificazione "con certezza" sarebbe senz'altro illegittima, portando una invalidità dei relativi certificati e delle conseguenti firme. Peraltro, l'adozione di procedure di identificazione più o meno sicure e rigorose, consente una differenziazione dei certificatori sul piano della fiducia ed affidamento che possono offrire al pubblico.

Inoltre, proprio per la sua importanza, la procedura di identificazione dovrebbe essere svolta direttamente dal certificatore (nell'ambito della sua struttura, ancorché decentrata) e non appare delegabile a soggetti diversi, che potrebbero introdurre elementi di incertezza difficilmente controllabili. In tal senso depone anche la lettura delle relative norme. In primo luogo, per l'art. 28 comma 2 lett. a T.U., "Il *certificatore* [e non altri] è tenuto a: a) identificare con certezza la persona che fa richiesta della certificazione"; per l'art. 22 comma 2 reg. tec., "il *certificatore* [e non altri] deve verificare l'identità del richiedente"; la facoltà data poi al certificatore di definire, pubblicandole nel manuale operativo, le "modalità di identificazione degli utenti" deve essere intesa come libertà nell'adozione di diverse procedure che nel rispetto dell'obiettivo della "identificazione con certezza", siano rivolte ad attività compiute dallo stesso certificatore e non da altri soggetti esterni delegati; per l'allegato II alla direttiva CE, "I *prestatori di servizi di certificazione* [e non altri] devono ... d) verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato". Nemmeno l'assunzione (implicita) di responsabilità da parte del certificatore per l'operato dei terzi delegati all'identificazione risolverebbe il problema, perché si tratta di garantire i terzi che verificano una firma circa l'identità del firmatario e l'efficacia del relativo atto, e non solo offrire una tutela di tipo risarcitorio.

In ogni caso, l'identificazione "con certezza" dovrebbe presupporre la presenza fisica del richiedente, restando escluse modalità di registrazione unicamente a distanza.

Considerando la novità della tecnologia e le responsabilità che ne possono derivare per gli utenti, in sede di registrazione, il certificatore è tenuto ad "informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi" (art. 28 comma 2 lett. e T.U.). Al momento della registrazione viene consegnato al titolare un dispositivo di firma, che viene personalizzato (art. 26 reg. tec.).

Dopo essere stato registrato, il titolare che intende ottenere la certificazione di una coppia di chiavi, deve inoltrare una richiesta al certificatore, in via telematica con il sistema di comunicazione sicuro previsto dall'art. 25 reg. tec., oppure con altro meccanismo previsto dal manuale operativo (art. 27 comma 1 reg. tec.). Le richieste di certificazione, unitamente alle richieste di registrazione, devono essere conservate dal certificatore per un periodo non inferiore a 10 anni (artt. 22 comma 1 e 27 comma 3 reg. tec.).

Con la richiesta, il titolare trasmette al certificatore la chiave pubblica di cui richiede la certificazione, se questa è stata generata autonomamente (art. 25 comma 1 lett. b reg. tec.). In caso di generazione effettuata dal certificatore (art. 7 reg. tec.), esso avrà già la disponibilità della chiave pubblica da certificare.

Prima di emettere il certificato, il certificatore deve (art. 28 comma 1 reg. tec.): "a) accertarsi dell'autenticità della richiesta; b) verificare che la chiave pubblica di cui si richiede la certificazione non sia stata certificata da uno dei certificatori iscritti nell'elenco; c) richiedere la prova del possesso della chiave privata e verificare il corretto funzionamento

della coppia di chiavi, eventualmente richiedendo la sottoscrizione di uno o più documenti di prova”.

Se le suddette verifiche risultano espletate con successo, il certificato viene generato in modalità di sicurezza e viene firmato digitalmente dal certificatore emittente utilizzando una chiave privata di certificazione (arg. *ex art.* 4 comma 4 lett. b reg. tec.).

Il certificato “deve essere pubblicato mediante inserimento nel registro dei certificati gestito dal certificatore” ed “il momento della pubblicazione deve essere attestato mediante generazione di una marca temporale” (art. 28 comma 4 reg. tec.).

A questo punto, solo dopo la pubblicazione il certificato viene inviato al titolare, insieme alla marca temporale che ne attesta la pubblicazione, (art. 28 comma 5 reg. tec.), in via telematica mediante il sistema di comunicazione sicuro di cui all'art. 25, oppure in altra modalità da definire (art. 45 comma 3 lett. i reg. tec.).

Il certificatore deve generare un certificato per ognuna delle proprie chiavi pubbliche di certificazione e firmarlo digitalmente con la chiave privata corrispondente a quella certificata (art. 19 comma 2 reg. tec.). Questi certificati sono comunicati all'AIPA (art. 17 comma 2 reg. tec.) e la loro lista, per ogni certificatore, è contenuta nell'elenco dei certificatori tenuto dall'AIPA stessa (art. 15 comma 1 lett. g reg. tec.). La stessa lista, sottoscritta dall'AIPA, deve essere mantenuta in copia e resa accessibile in via telematica dal relativo certificatore cui si riferisce (art. 17 comma 4 reg. tec.). Infine, tali certificati sono registrati nel dispositivo di firma del titolare, all'atto della sua personalizzazione (art. 26 comma 1 lett. b reg. tec.).

Ogni certificatore deve, inoltre, generare un certificato per ciascuna delle chiavi (pubbliche) di firma dell'AIPA e pubblicarlo nel proprio registro dei certificati (art. 17 comma 3 reg. tec.). “Per ciascuna coppia di chiavi [dell'AIPA] sono pubblicati sulla Gazzetta Ufficiale della Repubblica Italiana uno o più codici identificativi idonei per la verifica del valore della chiave pubblica” (art. 14 comma 2 reg. tec.).

Sembra che l'AIPA, inoltre, autocertifichi le proprie chiavi (arg. *ex art.* 39 comma 1 reg. tec.). Peraltro, “L’Autorità per l'informatica nella Pubblica Amministrazione può delegare la certificazione delle proprie chiavi al Centro Tecnico per l'assistenza ai soggetti che utilizzano la rete unitaria della pubblica amministrazione, istituito dall'articolo 17, comma 19, della legge 15 maggio 1997, n. 127” (art. 14 comma 1 reg. tec.). In effetti, le chiavi dell'AIPA sono certificate dal Centro tecnico ed i relativi codici identificativi costituiti dall'impronta del certificato della chiave pubblica stessa, sono stati resi noti con la circolare del 18 maggio 2001, n. 29.

“È consentito ai certificatori definire accordi di certificazione”, con cui “un certificatore emette a favore dell'altro un certificato relativo a ciascuna chiave di certificazione che viene riconosciuta nel proprio ambito” (art. 21 commi 1 e 2 reg. tec.). Ad es. il certificatore Beta genera un certificato per una chiave (pubblica) di certificazione di Alfa. In tal caso la verifica dei certificati di Alfa può essere compiuta contattando solo il certificatore Beta e non anche Alfa.

Per la fissazione delle caratteristiche e del contenuto del certificato, il T.U. rinvia alle regole tecniche, le quali stabiliscono che i certificati - relativi a tutte le tipologie di chiavi - debbano contenere obbligatoriamente (“almeno”) le seguenti informazioni (art. 11 reg. tec.):

- a) numero di serie del certificato;
- b) ragione o denominazione sociale del certificatore;
- c) codice identificativo del titolare presso il certificatore (art. 22 comma 3 reg. tec.);
- d) nome cognome e data di nascita ovvero ragione o denominazione sociale del titolare.

Questa indicazione può essere sostituita da uno pseudonimo, che deve essere esplicitamente indicato nel certificato (art. 23 comma 1 reg. tec.). In tal caso, “il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno 10 anni dopo la

scadenza del certificato” (art. 23 comma 2 reg. tec., vedi anche direttiva CE art. 8 comma 3, allegato I lett. c, allegato IV lett. f e considerando n. 25).

- e) valore della chiave pubblica;
- f) algoritmi di generazione e verifica utilizzabili;
- g) inizio e fine del periodo di validità delle chiavi;
- h) algoritmo di sottoscrizione del certificato.

Dal certificato deve, inoltre, potersi desumere in modo inequivocabile la tipologia della chiave certificata: di sottoscrizione, di certificazione, di marcatura temporale (art. 11 comma 2 reg. tec.).

Nei certificati relativi ad una chiave pubblica di sottoscrizione, in aggiunta alle informazioni suddette, possono, facoltativamente, essere indicati (art. 11 comma 3 reg. tec.):

a) eventuali limitazioni nell'uso della coppia di chiavi. Potrebbe stabilirsi che la relativa chiave privata non può essere utilizzata per la firma di documenti oltre un certo valore (ad es. di prezzo), oppure che non può essere utilizzata per certi tipi di atti (limitazione in negativo) o, infine, che può essere utilizzata solo per ben determinati tipi di atti (limitazione in positivo). Per la direttiva CE, “I certificati qualificati devono includere: [...] i) i limiti d'uso del certificato, ove applicabili; j) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili” (allegato I direttiva CE);

b) eventuali poteri di rappresentanza;

c) eventuali abilitazioni professionali. Il certificatore è tenuto a “specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite” (art. 28 comma 2 lett. c T.U.).

Il certificato non è un atto che produce una pubblica certezza, perché solo organi dello Stato o di enti pubblici o eccezionalmente esercenti privati di pubbliche funzioni possono porre in essere certezze pubbliche, e sempre in ipotesi tassativamente indicate. Il certificato non possiede, dunque, una fede privilegiata e non fa prova fino a querela di falso. Piuttosto, il contenuto di un valido certificato dovrebbe presumersi veritiero, efficace ed opponibile nei confronti del titolare (art. 22 lett. n T.U.), fino alla prova contraria, che può essere fornita senza la necessità di attivare un giudizio di querela di falso.

I certificati che contengono informazioni che non riguardano solo l'identità della persona, ma anche sue qualità ed attributi, sono detti certificati di attribuzione (*Authorizing Certificates*).

Non è escluso che il certificatore possa emettere dei certificati di attribuzione distinti ed in aggiunta al certificato base di identità. Potrebbero anche essere emessi più certificati di attribuzione in relazione alla stessa chiave pubblica ed allo stesso soggetto: ogni certificato indicherà un diverso potere, abilitazione, carica, titolo, ecc. Disporre di certificati di attribuzione distinti da quello base della chiave pubblica (di identità), consente di mantenere fermo quest'ultimo e modificare solo i primi a seguito di variazioni delle attribuzioni (ad es. promozione di un dipendente, aggiunta di funzioni, riduzione o estensione di poteri di rappresentanza, ecc.).

I certificati di attribuzione (*Attribute Certificates*) sono previsti dalla Raccomandazione X.509 dell'ITU (§ 13) e da alcune leggi straniere in materia. Non sono, invece, disciplinati espressamente dalla normativa italiana. Si pone quindi il problema dei requisiti di sicurezza applicabili e delle responsabilità cui andrebbero incontro i certificatori di attributo.

L'esigenza di riscontrare la cosiddetta qualifica o attribuzione, direttamente attraverso strumenti informatici *on-line* senza fare ricorso ai tradizionali mezzi e registri cartacei, si è posta in tutta la sua gravità per l'esercizio delle funzioni pubbliche in generale e più in particolare per le funzioni notarili. Il notaio, infatti, dovrà disporre di un certificato per

apporre firme digitali in sede di autenticazione di firme digitali *ex art.* 24 T.U. ed in sede di rilascio di copie conformi *ex art.* 20 T.U.

La firma digitale dovrebbe diventare un'occasione per elevare la sicurezza dei documenti e la fiducia di chi li riceve, piuttosto che condurre alla diffusione di un sistema con minori garanzie di quelle attuali. Nel sistema tradizionale, l'accertamento della legittimazione all'esercizio della funzione notarile da parte del pubblico deriva dall'esame e consultazione di una serie di fonti esterne al documento stesso. In primo luogo, la consultazione del ruolo dei notai presso il consiglio notarile distrettuale. Secondariamente, nella pratica quotidiana, attraverso una serie di elementi ed "indizi" empirici (ad es. presenza fisica ed "aspetto" del professionista, presentazione di altri, studio attrezzato, colloqui, esibizione del tesserino, ecc.). In caso di ricezione di un documento trasmesso telematicamente, non sono riscontrabili tutti i suddetti "indizi", e risulterebbe alquanto disagiata l'esame del ruolo presso il consiglio notarile. Pertanto, il ricorso a fonti unicamente extratestuali per la dimostrazione dell'attributo (funzione), renderebbe più difficile, rispetto alla pratica odierna, effettuare un tale riscontro ed abbasserebbe in definitiva il grado di sicurezza giuridica del documento, rischiando l'instaurarsi di un sistema la cui sicurezza sarebbe basata su verifiche solo a campione e successive.

In applicazione dell'art. 29 comma 3 T.U., secondo cui "Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici", il notariato sta istituendo una propria autonoma infrastruttura di certificazione, con la collaborazione tecnica della società "Notartel s.p.a.". Il Consiglio Nazionale del Notariato (CNN) sarà iscritto quale certificatore nell'apposito elenco pubblico tenuto dall'AIPA. (art. 27 comma 3 T.U.). Il rinvio che il citato art. 29 T.U. effettua all'ordinamento del notariato, impone, infatti, il riscontro del cosiddetto "attributo", cioè l'effettiva ed attuale iscrizione del notaio (titolare della chiave) nel ruolo dei notai del relativo distretto, tenuto conto non solo di eventuali sospensioni o cessazioni transitorie, ma anche del limite territoriale di competenza del notaio (art. 27 l. not.). Poiché tale attestazione è per legge di competenza esclusiva del presidente del consiglio notarile distrettuale di appartenenza, si pensa che il rilascio delle chiavi dovrà svolgersi mediante una previa procedura che coinvolga, tramite il CNN, lo stesso presidente in sede di consegna materiale del dispositivo di firma e di eventuale revoca o sospensione del certificato. Le comunicazioni sicure tra le sedi decentrate (i distretti) ed il certificatore (il CNN) avverranno attraverso la Rete Unitaria del Notariato (RUN). La chiave così rilasciata al notaio, potrà essere utilizzata solo per apporre firme digitali collegate all'esercizio della funzione pubblica, un po' come oggi è limitato l'uso del sigillo, salvo casi che saranno espressamente autorizzati dal CNN. La verifica delle firme digitali dei notai con i relativi attributi dovrà essere accessibile a chiunque, prelevando telematicamente dal sito del certificatore CNN i relativi certificati, con le liste di revoca o sospensione. Per la soluzione del problema del controllo dell'"attributo" di notaio, si sono prospettate tre soluzioni tecniche alternative: a) certificato di attributo (distinto dal certificato di firma) rilasciato dal CNN; b) certificato di firma contenente un'estensione (critica – cioè non ignorabile dal *software* di verifica) che indica la funzione di notaio, rilasciato con la necessaria partecipazione del CNN e dei consigli distrettuali; c) certificato di firma semplice rilasciato dal CNN esclusivamente ai notai in esercizio, sulla base di apposita restrizione prevista nel manuale operativo. La consultazione di semplici registri *on-line* contenenti gli elenchi dei notai in esercizio, per dare effettive garanzie, dovrebbe fornire risposte nella forma di documenti informatici con una firma digitale del soggetto autorizzato a certificare la funzione di notaio (il presidente del consiglio notarile distrettuale) e, pertanto, si ritornerebbe sostanzialmente al sistema del certificato di attributo.

Si ricorda che nel sistema italiano, il notaio non è soggetto che certifica le chiavi pubbliche con gli effetti di cui al T.U., essendo tale compito riservato ai certificatori *ex art. 27 T.U.* Il notaio, invece, come detto sopra, può “certificare” la fase della concreta apposizione della firma digitale, secondo la procedura dell’autenticazione *ex art. 24 T.U.* Peraltro, nella fase di registrazione degli utenti per l’emissione del certificato (*identity certificate*), al fine di raggiungere un maggiore e documentato grado di certezza dell’identità personale, il certificatore potrebbe richiedere, in aggiunta ai suoi accertamenti, l’autenticazione notarile della sottoscrizione apposta nel contratto di certificazione. Ai sensi delle regole tecniche, infatti, “È data facoltà al certificatore di definire, pubblicandole nel manuale operativo, le modalità di identificazione degli utenti” (art. 22 comma 3 reg. tec.).

I certificati delle chiavi di sottoscrizione sono resi pubblici dal certificatore emittente (art. 23 comma 7 T.U., art. 27 comma 2 T.U.) mediante inserimento nel registro dei certificati (*key repository*) gestito dal certificatore stesso (art. 28 comma 4 reg. tec.), ed “accessibile a qualsiasi soggetto” (art. 43 comma 4 reg. tec.). Il registro dei certificati, da istituire e gestire (art. 45 comma 3 lett. o reg. tec.) da parte di ciascun certificatore, con modalità di sicurezza, dovrà contenere: “a) i certificati emessi dal certificatore; b) la lista dei certificati revocati; c) la lista dei certificati sospesi” (art. 43 comma 1 reg. tec.). Le liste dei certificati revocati e sospesi possono essere suddivise in più liste distinte (art. 43 comma 2 reg. tec.), per non appesantire la gestione con enormi liste di vecchi certificati.

L’accesso ai registri dei certificati avviene in via telematica secondo modalità tecniche standard (art. 13 reg. tec.), definite anche nel manuale operativo (art. 45 comma 3 lett. o reg. tec.). L’autenticità di queste liste è garantita dalla firma digitale apposta con una chiave di certificazione dal certificatore che le gestisce (art. 4 comma 4 lett. b reg. tec.).

Il momento della pubblicazione del certificato nel registro deve essere attestato mediante generazione di una marca temporale, “che deve essere conservata fino alla scadenza della validità della chiavi” (art. 28 comma 4 reg. tec.).

Le “chiavi pubbliche di cifratura [con i relativi certificati] sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro validità, sono consultabili in forma telematica” (art. 27 comma 2 T.U.). Non è escluso che il certificatore si impegni nel manuale operativo (art. 45 reg. tec.) alla custodia dei certificati per un periodo di tempo superiore. Il termine di custodia del certificato è superiore al termine di scadenza (che non può essere in ogni caso superiore a tre anni, art. 22 lett. f T.U.) per consentire di verificare firme digitali anche dopo la scadenza del certificato stesso, con un termine identico a quello ordinario di prescrizione (art. 2946 c.c.).

1.7 La perdita di validità dei certificati

Il T.U. stabilisce che “Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa” (art. 23 comma 4 T.U.); si intende “per validità del certificato, l’efficacia, e l’opponibilità al titolare della chiave pubblica, dei dati in esso contenuti” (art. 22 lett. n T.U.), cioè fondamentalmente il legame tra identità personale e chiave pubblica, nonché (se specificati) i poteri di rappresentanza, cariche o abilitazioni professionali.

La perdita di validità del certificato relativo ad una chiave di sottoscrizione può derivare da scadenza, revoca o sospensione.

Il certificato deve indicare “inizio e fine di validità delle chiavi” (art. 11 comma 1 lett. g reg. tec.). Il termine di scadenza di un certificato non può, comunque, essere superiore a 3 anni (art. 22 lett. f T.U.); ma può essere stabilito un termine inferiore. “Il soggetto certificatore determina il termine di scadenza del certificato ed il periodo di validità delle chiavi in funzione degli algoritmi impiegati, della lunghezza delle chiavi e dei servizi cui esse sono destinate” (art. 4 comma 7 reg. tec.).

La predeterminazione di un termine di scadenza si giustifica per le seguenti ragioni: a) progresso nella velocità dell'*hardware* (secondo la regola d'esperienza, detta "legge di Moore", la potenza di calcolo disponibile allo stesso costo raddoppia ogni 18 mesi) e negli algoritmi per la soluzione dei problemi matematici di base (come la fattorizzazione), per cui chiavi un tempo sicure ad attacchi esaustivi o analitici, possono non esserlo più; b) riduzione delle informazioni a disposizione del crittoanalista, dato che ogni volta che una chiave è utilizzata si generano delle informazioni (testo cifrato) che possono agevolare la ricerca da parte del crittoanalista; c) minimizzazione degli eventuali danni derivanti dalla compromissione della chiave a seguito di smarrimento o di individuazione da parte del crittoanalista. Pertanto, chiavi maggiormente sicure (perché più lunghe) possono avere un termine di scadenza superiore rispetto a chiavi con un livello di sicurezza minore.

Prima della scadenza, una chiave (ed il relativo certificato) può perdere validità per revoca o sospensione.

Il T.U. definisce "per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi" (art. 22 lett. l T.U.); "per sospensione del certificato, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo" (art. 22 lett. m T.U.); e prevede che il certificatore deve provvedere "alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni" (art. 28 comma 2 lett. h T.U.).

La revoca e la sospensione sono effettuate dal certificatore emittente, a seguito di richiesta del titolare, del terzo interessato o su iniziativa dello stesso certificatore (artt. 29 comma 2 e 33 comma 1 reg. tec.).

Il titolare può richiedere la revoca o sospensione, inoltrando una richiesta "redatta per iscritto", specificandone la motivazione e la sua decorrenza (per la revoca) o il periodo di sospensione (artt. 31 comma 1 e 35 comma 1 reg. tec.). Il titolare ha un vero e proprio obbligo di "richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi" (art. 8 comma 4 reg. tec.). La richiesta viene inoltrata in via telematica attraverso il sistema di comunicazione sicuro predisposto all'atto della registrazione o con altre modalità alternative previste nel manuale operativo (artt. 31 commi 2-3 e 35 commi 2-3 reg. tec.). Prima di procedere alla revoca o sospensione, il certificatore deve verificare l'autenticità della richiesta. Se tale accertamento non può essere compiuto in tempo utile, in attesa della revoca definitiva, è stabilito che si proceda alla sospensione (art. 32 reg. tec.).

La revoca e la sospensione del certificato sono effettuate dal certificatore mediante l'inserimento, rispettivamente, in una delle liste di certificati revocati (*Certificate Revocation Lists*, CRL), o in una delle liste di certificati sospesi (*Certificate Suspension Lists*, CSL), da esso gestite (artt. 29 comma 3 e 33 comma 2 reg. tec.). Queste liste sono contenute nel registro dei certificati (art. 43 reg. tec.), che è accessibile telematicamente (art. 13 reg. tec.). Come si desume dall'art. 1 comma 4 lett. b reg. tec., le liste di revoca e di sospensione sono firmate digitalmente dal certificatore, applicando una chiave (privata) di certificazione.

La revoca di un certificato determina la cessazione anticipata della sua validità (art. 29 comma 1 reg. tec.). L'efficacia della revoca e della sospensione decorre solo dal momento di pubblicazione della relativa lista (art. 23 comma 5 reg. ed artt. 29 comma 3 e 33 comma 2 reg. tec.), che deve essere asseverato mediante l'apposizione di una marca temporale (artt. 29 comma 4 e 33 comma 2 reg. tec.). Questa pubblicazione deve essere compiuta dal certificatore "tempestivamente" (art. 28 comma 2 lett. h T.U.), potendo altrimenti essere ritenuto responsabile del danno che il ritardo ha cagionato al titolare della chiave, per

eventuali affidamenti riposti dai terzi. In particolare, se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, oppure se è chiesta una sospensione per la stessa causa, è prescritto che il certificatore deve procedere immediatamente alla relativa pubblicazione (artt. 29 comma 5 e 34 comma 3 reg. tec.).

Nelle more tra la richiesta e la pubblicazione, si ammette una limitata forma di “pubblicità di fatto”, per cui, è consentito (con l’onere a carico del revocante o di chi richiede la sospensione) provare che la revoca o sospensione erano già a conoscenza delle parti interessate, anche in mancanza (o prima) della necessaria pubblicazione (art. 23 comma 5 T.U.). Tale prova, però, letteralmente, sembra poter sostituire solo la mancata (o ritardata) pubblicazione, ma non anche la mancata previa *richiesta* di revoca o sospensione al certificatore stesso; inoltre, sembra che non sia consentito dimostrare la semplice conoscibilità della revoca o sospensione, cioè l’ignoranza dipendente da colpa, ma sia indispensabile dimostrare la effettiva “conoscenza”.

Comunque, non sembra possibile invocare la mancata conoscenza di fatto, in contrasto con le risultanze del registro dei certificati. Quest’ultimo dato, consentirebbe di attribuire in qualche misura al registro dei certificati la funzione della pubblicità legale, caratterizzata proprio da questo effetto di conoscibilità legale, di surrogato della conoscenza.

Le modalità di sospensione e revoca dei certificati sono, inoltre, precisate nel manuale operativo del certificatore (art. 45 comma 3 lett. I reg. tec.).

Una firma digitale apposta o associata “mediante una chiave [privata] revocata, scaduta o sospesa [e correttamente pubblicata] equivale a mancata sottoscrizione” (art. 23 comma 5 T.U.). Mancando la sottoscrizione, il valore giuridico sarà quello di mero documento informatico non sottoscritto.

Qualora la forma scritta è richiesta *ad substantiam*, il relativo atto giuridico è nullo o inesistente; qualora la forma scritta è richiesta solo *ad probationem*, rimane il limite alla prova testimoniale (art. 2725 c.c.) e per presunzioni (art. 2729 comma 2 c.c.), ma l’atto può essere provato con la confessione o il giuramento. In caso di atti bi- o plurilaterali, o che possono produrre effetti nella sfera giuridica altrui, nessun affidamento incolpevole, risarcimento o indennizzo può essere riconosciuto in capo alla controparte o al terzo, i quali hanno la possibilità e l’onere di consultare i registri telematici dei certificatori per informarsi sulla validità della chiave.

La scadenza, revoca o sospensione della chiave non produce la perdita di validità delle relative firme digitali con essa verificabili, solo se può essere dimostrata la anteriorità delle firme stesse rispetto alla perdita di validità della chiave (art. 60 reg. tec.), mediante marcatura temporale o altro strumento. In tal senso limitato va intesa la non retroattività della revoca, prevista dall’art. 22 lett. I T.U.

2 IL VALORE GIURIDICO DELLA FIRMA DIGITALE

2.1 Il documento informatico

Il “documento informatico” è definito come “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” (art. 1 lett. b T.U.). Tale definizione riproduce sostanzialmente, con l’aggiunta del termine “informatica”, quella che da tempo era già stata elaborata dalla dottrina - e che non è mai stata prima recepita dal legislatore - per individuare il concetto di documento (non ancora informatico).

Un documento informatico può rappresentare qualunque tipo di informazione (testi, immagini, suoni, animazioni grafiche, ecc.), purché sia digitalizzata, cioè rappresentata tramite valori numerici (*digit*).

La definizione del T.U. prescinde da qualunque riferimento ad un “supporto” materiale, a differenza della definizione data dall’art. 491 *bis* c.p., introdotto dalla legge 23 dicembre 1993, n. 547, per il quale è documento informatico “qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli” (lo stesso per l’art. 621 c.p.).

Il documento informatico, come sopra definito, prescinde dalla sussistenza di una firma digitale o, più in generale, elettronica. D'altra parte, l'art. 23 comma 1 T.U. prevede che al documento informatico “può essere apposta” una firma digitale, senza cioè prescriverne l'obbligatorietà, salvo la diversa validità ed efficacia probatoria che ne risulta.

Peraltro, un documento informatico di per sé, privo di firma digitale o, più in generale, di una firma elettronica, in ragione delle sue caratteristiche tecniche, non consente alcuna verifica né della sua provenienza soggettiva, né della sua integrità di contenuto. Il documento informatico, infatti, non può evidentemente essere sottoscritto in modo tradizionale, mediante apposizione autografa del nome e cognome dell’autore o di chi ne assume la paternità; il supporto informatico, non possiede le caratteristiche proprie dei supporti tradizionali come la carta, poiché le registrazioni effettuate sono di norma non indelebili e non consentono la riconoscibilità di eventuali alterazioni del suo contenuto (accidentali o intenzionali).

Dalle caratteristiche di sicurezza di un certo tipo di documento ne deriva il suo trattamento giuridico in termini di logica ed imprescindibile consequenzialità. Così, il documento scritto cartaceo, in ragione della possibilità di accertarne l’integrità e la provenienza - in modi più o meno sicuri - attraverso perizie scientifiche e grafologiche sul supporto e sulla sottoscrizione, ha da parte del legislatore una marcata preferenza rispetto ad altre prove (ad es. orali); preferenza che nel codice del 1942 si manifesta nel valore probatorio riconosciuto alla scrittura privata (artt. 2702-2704 c.c.) ed all’atto pubblico (art. 2699-2701 c.c.).

L’obiettivo del regolamento emanato con D.P.R. n. 513/1997 (ora trasfuso nel T.U.) e dei successivi provvedimenti di attuazione, è il pieno riconoscimento giuridico della documentazione informatica e la sua equiparazione alla tradizionale documentazione cartacea, come si desume dalla delega contenuta nell’art. 15 comma 2 della legge 15 marzo 1997, n. 59 (c.d. legge Bassanini-uno). La firma digitale disciplinata da tali provvedimenti, nel quadro di stringenti requisiti di sicurezza in una complessa infrastruttura di certificazione minuziosamente delineata, consente, dunque, la produzione di documenti informatici del tutto parificati agli effetti giuridici a documenti già noti e previsti dal codice civile.

Le difficoltà, che impedivano il riconoscimento di una piena efficacia probatoria del documento informatico, sono state superate con l’impiego delle tecnologie di cifratura dei dati che, mediante l’apposizione di firme digitali, consentono di riprodurre nel documento informatico, per un verso quelle che sono state considerate le funzioni tipiche della sottoscrizione, per un altro verso le risultanze in termini di verifica dell’integrità che sono proprie di un supporto cartaceo.

La firma digitale “italiana” conforme al T.U. rientra nell’ambito della c.d. “firma elettronica avanzata”, di matrice comunitaria, definita e disciplinata dalla già citata direttiva del 13 dicembre 1999, n. 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche. La direttiva CE, basata sui principi della neutralità tecnologica, della libertà di accesso al mercato dei servizi di certificazione, e del riconoscimento del valore giuridico delle firme elettroniche, dovrà essere attuata nell’ordinamento italiano, con l’introduzione di nuove norme e la modifica di alcune norme già esistenti del T.U. (il termine scadeva il 19 luglio 2001) Peraltro, anche allo stato attuale, in attesa dell’attuazione della direttiva, nel nostro ordinamento non è certo proibito fare uso di firme elettroniche, diverse dalla firma digitale pienamente conforme al T.U.

Pertanto, la sottoscrizione elettronica dei documenti informatici opera (ed opererà a seguito dell'attuazione della direttiva CE) su un doppio binario: a) firme digitali (firme elettroniche avanzate), parificate alla sottoscrizione tradizionale, e basate su minuziose prescrizioni di sicurezza per la loro implementazione; b) firme elettroniche *tout court*, non parificate alla sottoscrizione tradizionale, ma non per questo prive di ogni valore giuridico, di libera implementazione nel quadro della direttiva comunitaria.

Sotto un altro profilo, le firme elettroniche la cui efficacia è basata su norme di legge, e come tali valide *erga omnes*, si contrappongono alle firme elettroniche la cui efficacia è basata su accordi contrattuali, e come tali valide solo tra le parti dell'accordo stesso. Accordi di tal genere, sotto il profilo probatorio rientrerebbero nella previsione dell'art. 2698 c.c. in quanto costituirebbero un'inversione convenzionale dell'onere della prova, ponendo una presunzione *juris tantum*, riguardante il fatto che una firma digitale - e quindi il documento informatico "sottoscritto" - è da considerarsi come proveniente dal soggetto collegato alla chiave pubblica utilizzata per la verifica. Di conseguenza, è quest'ultimo soggetto che, dopo la verifica positiva della sua firma digitale in giudizio, è tenuto a fornire l'eventuale prova a discarico. Sotto altro profilo tali accordi rientrerebbero nell'art. 1469 *bis* n. 17 c.c., che presume vessatorie le clausole che, tra l'altro, sanciscono a carico del consumatore limitazioni della facoltà di apporre eccezioni, limitazioni all'allegazione di prove, inversioni o modificazioni dell'onere della prova. Dal punto di vista della forma, questi accordi potrebbero essere inquadrati nell'art. 1352 c.c., disciplinante le forme convenzionali. Comunque, trattandosi di firme non conformi al regolamento, non sarebbero idonee ad integrare i requisiti di forma richiesti dalla legge *ad substantiam* o *ad probationem*.

La direttiva europea non disciplina le firme elettroniche della seconda specie, la cui efficacia non è basata su un sistema normativo, ma è basata esclusivamente all'interno di sistemi fondati su accordi volontari di diritto privato fra un numero determinato di partecipanti (gruppi chiusi di utenti). Come si legge nel considerando n. 16 alla direttiva CE, "nella misura consentita dal diritto nazionale, andrebbe rispettata la libertà delle parti di accordarsi sulle condizioni di accettazione dei dati firmati in modo elettronico; alle firme elettroniche utilizzate in tali sistemi non dovrebbero essere negate l'efficacia giuridica e l'ammissibilità come mezzo probatorio nei procedimenti giudiziari".

In relazione alle prescrizioni giuridiche di forma minima, alle esigenze concrete, alle garanzie richieste, all'ammontare degli interessi in gioco, ci si potrà servire di firme digitali o di semplici firme elettroniche. Ad es. l'acquisto di un libro su Internet e, più in generale, gran parte dell'odierno commercio elettronico B2C (*Business to Consumer*) in Internet, non richiede forme minime e sarebbe già abbastanza garantito da semplici firme elettroniche; l'acquisto di un appartamento o la copia di un atto da trasmettere a pubblici registri richiede, invece, la forma minima del documento informatico con firma digitale conforme (firma elettronica avanzata), che potrà essere applicata in ogni altro caso in cui, a prescindere da prescrizioni normative, si ritenga un'opportuna garanzia.

2.2 Il documento informatico con firma digitale

La dottrina italiana anteriore al D.P.R. n. 513/1997, pur considerando il documento informatico come documento scritto, aveva quasi unanimemente negato la configurabilità di una scrittura privata (art. 2702 c.c.) in forma informatica, per l'impossibilità di apporvi l'elemento essenziale della sottoscrizione.

Nel disciplinare l'efficacia probatoria e la struttura del documento informatico, il D.P.R. n. 513/1997 (ora T.U.) segue una prospettiva di simmetria con la corrispondente documentazione cartacea come disciplinata dal codice civile. Secondo la Relazione al D.P.R. n. 513/1997 predisposta dall'AIPA, "il criterio adottato, per la formulazione delle norme autorizzate, consiste nel tentativo di adattare le norme vigenti (in particolare la disciplina in

materia di efficacia probatoria degli atti e dei documenti del codice civile) alle nuove realtà informatiche e telematiche”. Questa tecnica, apprezzabile per l’impostazione di fondo, ha determinato però, come si vedrà, notevoli dubbi interpretativi, per la obiettiva difficoltà di applicare alla nuova fattispecie del documento informatico delle norme pensate e scritte per il diverso tipo di documentazione cartacea.

Il T.U. così stabilisce 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” (art. 23 comma 2 T.U.). Si badi bene che la firma digitale non “è” una sottoscrizione, ma “equivale” alla sottoscrizione. Dall'equivalenza tra firma digitale e sottoscrizione deriva la sostituibilità della prima alla seconda, in tutte quelle norme esistenti che fanno espresso riferimento alla sottoscrizione. Inoltre, è stabilito che la firma digitale sostituisce l'apposizione di “sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere” (art. 23 comma 7 T.U.), che ovviamente non potrebbero essere apposti su un documento immateriale come quello informatico, ma solo eventualmente sul contingente “supporto” informatico.

In relazione alle disposizioni della direttiva comunitaria, sotto questo aspetto, il T.U. si può già ritenere sostanzialmente conforme. Come si è detto, la firma digitale “italiana” corrisponde ad una “firma elettronica avanzata” di matrice comunitaria. Sul piano dell’efficacia giuridica, la direttiva impone agli Stati membri di parificare le “firme elettroniche avanzate” alle sottoscrizioni su carta, più precisamente riconoscendo alle “firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura” i “requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei” e che “siano ammesse come prova in giudizio” (art. 5 direttiva CE).

Il basilare principio di “equivalenza” tra firma digitale e sottoscrizione cartacea posta dall'art. 23 comma 2 T.U. conduce di conseguenza all’attribuzione al documento informatico della stessa efficacia probatoria tradizionalmente riconosciuta al documento cartaceo nelle sue varie forme. In tal senso, si stabilisce che “Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile” (art. 10 comma 3 T.U.).

Attribuire al documento informatico l’efficacia probatoria di scrittura privata, comporta che esso “fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta” (art. 2702 c.c.).

Nel codice civile l’efficacia di piena prova della scrittura privata, che vincola il giudizio alle sue risultanze (in deroga al principio del libero convincimento del giudice espresso dall'art. 116 c.p.c.) deriva da tre circostanze alternative: riconoscimento, giudizio positivo di verifica, autenticazione. In caso di riconoscimento (*rectius* mancato disconoscimento entro i termini) da parte di colui indicato come autore, la scrittura privata forma piena prova. In caso di disconoscimento, la parte che produce il documento può chiedere il giudizio di verifica (artt. 216 ss. c.p.c.). L’oggetto della verifica consiste nella falsità (materiale) della dichiarazione documentata e della sottoscrizione, essendo finalizzato esclusivamente a stabilire che il documento non è stato alterato e se la sottoscrizione è stata apposta o no da chi figura come sottoscrittore. In tale giudizio incidentale l’onere della prova spetta a chi ha prodotto la scrittura. L’esito positivo del giudizio di verifica porta alla stessa efficacia probatoria ottenibile con il riconoscimento (piena prova).

Una volta che (a seguito di riconoscimento o verifica) la scrittura privata acquisisce efficacia di piena prova, tale efficacia può essere contestata – secondo un’attendibile ricostruzione - tramite il procedimento di querela di falso del documento (artt. 221 ss. c.p.c.).

In esso, l'onere della prova spetta a colui che risulta sottoscrittore (art. 221 comma 2 c.p.c.), determinandosi così normalmente un'inversione rispetto al giudizio di verifica.

Questi istituti devono essere applicati, con opportuni adattamenti, al documento informatico, in quanto l'art. 10 comma 3 T.U. opera un rinvio all'art. 2702 c.c. nella sua interezza.

Innanzitutto, il documento informatico con firma digitale potrebbe essere riconosciuto, assumendo fin da subito l'efficacia di piena prova. Il riconoscimento non dovrebbe escludere la necessità che si proceda, comunque, ad una verifica tecnica della firma digitale, cioè verifica della corrispondenza con una chiave pubblica validamente certificata.

In caso di disconoscimento, la controparte potrebbe chiederne la verifica. Ammettendo il giudizio di verifica, si tratta di individuarne l'oggetto della prova: cioè se esso consista nell'individuazione del reale autore della firma (colui che ha utilizzato il dispositivo di firma), oppure più semplicemente nella verifica tecnica della firma e nell'individuazione del soggetto titolare del relativo certificato.

a) Seguendo la prima ricostruzione (giudizio di verifica quale sede per accertare il reale autore della firma digitale), a seguito della verifica tecnica con un valido certificato, si dovrebbe, comunque, muovere dalla presunzione di riferibilità della firma in capo al soggetto che risulta titolare del relativo certificato e dalla presunzione di veridicità ed esattezza di quest'ultimo (se conforme a tutte le norme). A seguito di verifica tecnica positiva, il soggetto che risulta titolare del relativo certificato avrebbe, nella stessa sede del giudizio di verifica, il difficile onere di dimostrare eventualmente di non essere il reale autore della firma generata con la chiave privata corrispondente a quella pubblica certificata a suo nome. Tale indagine sarebbe totalmente extradocumentale, non avendo la firma digitale la capacità di dare indicazioni sul suo reale autore. Ragionando diversamente, cioè escludendo che si verificano le dette presunzioni, si porrebbe a carico di chi produce la scrittura (documento informatico) un onere probatorio eccessivamente gravoso e contro i principi, che vanificherebbe il meccanismo della firma digitale e dell'infrastruttura a chiave pubblica. La semplice titolarità di un certificato di chiave pubblica con cui si verifica una firma digitale comporterebbe dunque di per sé una presunzione di responsabilità e riferibilità di tutte le firme con esso verificabili.

b) Seguendo la seconda ricostruzione (giudizio di verifica quale sede di un'indagine esclusivamente di carattere tecnico sulla decifrabilità con la chiave pubblica e sulla validità del certificato), la parte attrice si limiterà a chiedere, come sopra, la verifica tecnica della firma, senza però che al soggetto presunto firmatario sia, poi, possibile dimostrare il contrario nella stessa sede del giudizio di verifica. In tal modo, la verifica, tuttavia, perderebbe sostanziale significato, riducendosi alla verifica tecnica della firma: un'operazione matematica oggettiva effettuabile immediatamente da chiunque disponga della semplice attrezzatura *hardware* e *software* necessaria.

Se la questione circa il reale autore della firma (in contrapposizione alla risultanza della verifica tecnica con il certificato) non poteva essere posta nel giudizio di verifica, diventa giocoforza ammetterla in sede di successiva querela di falso, per non lasciare il titolare della chiave privo di tutela ed esporlo ad una forma di responsabilità oggettiva. L'oggetto del giudizio di querela di falso per il documento informatico con firma digitale, consisterà nello stabilire chi sia l'effettivo soggetto (autore) che ha apposto la firma utilizzando la chiave. Oppure, più semplicemente, consisterà nello stabilire che il reale autore della firma sul documento informatico in questione non è il titolare della relativa chiave certificata. Non si tratta, dunque di provare la "falsità" della firma (come differente da un preteso modello somatico), dato che la firma generata sullo stesso documento con la stessa chiave è indistinguibile anche se la chiave è utilizzata da soggetti diversi dal titolare; bensì l'"abuso" nell'utilizzo della relativa chiave privata. A colui che è risultato titolare della chiave

(a seguito della verifica) spetta il difficile onere di provare il contrario, utilizzando ogni mezzo. I mezzi di prova nell'ambito della querela di falso sono liberi, consistendo in quelli ordinari del nostro sistema probatorio (prove testimoniali, presunzioni, confessione, ecc.).

In conclusione, questi problemi si pongono perché la firma digitale *ex art. 23 T.U.* non è in grado di rappresentare il suo reale autore, ma solo il soggetto titolare del relativo certificato da utilizzare per la verifica tecnica. La chiave privata è, infatti uno strumento tecnico che può essere, astrattamente, utilizzato da chiunque, a differenza della sottoscrizione autografa che è una risultanza a carattere esclusivamente personale. Si pensi ad es. alle ipotesi di smarrimento o sottrazione del dispositivo di firma. A seguito della verifica tecnica della firma, resta perciò incerto il soggetto che ha realmente apposto la sottoscrizione, utilizzando materialmente il dispositivo di firma.

Non potendo tecnicamente risultare alcuna prova circa il soggetto reale autore della sottoscrizione, l'unico sistema per attribuire efficacia probatoria a tali firme è il ricorso a dei meccanismi presuntivi di responsabilità in capo al titolare della chiave come risulta dal certificato. Dalla titolarità di un certificato deriverebbe una presunzione (*iuris tantum*) di provenienza delle firme digitali con esso verificabili in capo al titolare medesimo. Dalla verifica di una firma digitale non risulterebbe dunque l'autore di essa, bensì più correttamente soltanto il soggetto che è responsabile per la firma apposta. Per la diffusione generalizzata del sistema diventano indispensabili adeguati contrappesi assicurativi a garanzia dei titolari delle chiavi, analogamente a quanto accade oggi per le carte di credito.

2.3 Il documento informatico con firma elettronica

La direttiva CE, in relazione alle semplici “firme elettroniche” (non avanzate), stabilisce che gli Stati membri “provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio” (art. 5 direttiva CE), lasciando così agli Stati membri determinare la misura di tale efficacia probatoria.

La vigente normativa italiana richiederebbe un adeguamento sotto tale profilo, in quanto non disciplina firme elettroniche diverse dalla firma digitale, però, come si è già rilevato, non ne proibisce l'uso. In attesa di conoscere il testo definitivo del decreto di attuazione della direttiva, si può tentare una ricostruzione teorica che tenga conto del sistema in cui la “firma elettronica” si dovrà incardinare.

Nella vigenza del D.P.R. n. 513/1997, si poteva sostenere che una firma digitale non conforme alle norme, oppure più in generale una “firma elettronica” intesa nel senso della direttiva CE, rientrasse nell'ambito applicativo dell'art. 2712 c.c. disciplinante le riproduzioni meccaniche. L'art. 5 comma 2 del D.P.R. n. 513/1997 stabiliva che “il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile”, accogliendo una delle tesi dottrinali più seguite. La norma poneva problemi interpretativi in relazione al senso da dare ai “requisiti” richiesti, però non richiedeva espressamente la sussistenza di una firma digitale. Pertanto, la dottrina da più parti era arrivata alla conclusione che il documento informatico, anche se privo di firma digitale o, comunque, con una firma digitale non conforme, potesse avere l'efficacia probatoria di riproduzione meccanica. D'altra parte, non avrebbe avuto senso assegnare l'efficacia *ex art. 2712 c.c.* solo al documento con firma digitale, quando a questo è attribuito già il valore superiore ed assorbente di scrittura privata (art. 5 comma 1 D.P.R. n. 513/1997). Dove è richiesta la firma digitale per l'attribuzione di una certa efficacia probatoria, ciò era espresso inequivocabilmente. Esclusa, dunque, la necessità di una firma digitale, non si vedeva quali altri requisiti potessero essere richiesti per integrare l'efficacia *ex art. 2712 c.c.*

Questa ricostruzione è stata recentemente confermata dalla sentenza Cass. Sez. lavoro 6 settembre 2001, n. 11445/2001, secondo cui i “documenti informatici, come quello rilevante in causa, privi di firma digitale, ... hanno l'efficacia probatoria prevista dall'art. 2712 cod. civ.

(art. 5, comma 2), come già ritenuto dalla dottrina e dalla giurisprudenza, nel senso che essi vanno ricondotti tra le riproduzioni fotografiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica (ed ora elettronica) di fatti e di cose, le quali 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. Nella interpretazione ed applicazione di tale norma, occorre tenere presente il consolidato insegnamento di questa Corte, secondo cui il disconoscimento della conformità di una delle riproduzioni menzionate nell'art. 2712 cod. civ. ai fatti rappresentati non ha gli stessi effetti del disconoscimento previsto dall'art. 215, comma secondo, cod. proc. civ., della scrittura privata, perché, mentre quest'ultimo, in mancanza di richiesta di verifica 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”.

Il nuovo T.U., che per altro ripropone quasi letteralmente le disposizioni del D.P.R. n. 513/1997, su questo punto si discosta, invece, in modo sostanziale. La nuova formulazione (art. 10 comma 1 T.U.) richiede, infatti, la sussistenza di una firma digitale ai fini dell'attribuzione di efficacia *ex art. 2712 c.c.* Peraltro, il documento informatico sottoscritto con “firma digitale” ha pure l'efficacia di scrittura privata, come stabilisce il successivo comma 3 dello stesso articolo. Allora, si pone l'alternativa: il documento informatico con firma digitale vale come riproduzione meccanica o come scrittura privata? Forse una chiave di lettura potrebbe essere quella del contenuto della rappresentazione digitale: se testuale, scrittura privata; se multimediale, riproduzione meccanica. Ma così ragionando, si escluderebbe che possano essere sottoscritti con effetti di scrittura privata – e, quindi, di cosiddetto non ripudio - alcuni tipi di documenti digitali, operando una limitazione arbitraria del concetto di documento informatico definito all'art. 1 T.U., la cui definizione non è ristretta a rappresentazioni testuali, ma genericamente “informatiche”, cioè digitali. Poiché il documento informatico (art. 1 lett. b T.U.) è idoneo ad essere rappresentato non solo per testi, ma anche immagini, filmati, suoni ed in generale qualunque informazione digitalizzabile, ne deriva la astratta configurabilità di documenti non testuali con efficacia di scrittura privata. Applicando letteralmente le norme del T.U. sarebbe difficile negare che ha efficacia di scrittura privata *ex art. 10* e soddisfi così letteralmente e sostanzialmente i requisiti richiesti dall'art. 1350 c.c., un documento informatico (eventualmente anche autenticabile *ex art. 24*), recante la registrazione digitale audio e video (completabile pure con elementi testuali) della conclusione di un negozio (eventualmente da trascrivere mediante indicizzazione non automatica del contenuto).

D'altra parte rimane il dubbio (non chiarito nemmeno dal codice civile e dal codice di procedura civile) se alla riproduzione meccanica disconosciuta è applicabile un qualche procedimento di verifica; procedimento che, in presenza di una firma digitale conforme al T.U. ed alle regole tecniche, sarebbe facilmente esperibile. Ma, così come si è sostenuto per il documento informatico scrittura privata, allo stesso modo, si potrebbe anche sostenere che non avrebbe addirittura senso parlare di un disconoscimento di riproduzione meccanica, qualora questa è garantita da una firma digitale conforme.

Peraltro, potrebbe sostenersi che la norma dell'art. 10 comma 1 T.U. come sopra esaminata, non dovrebbe, comunque, escludere che l'art. 2712 c.c., in virtù della sua ampia formulazione, possa essere applicato in via diretta (e non solo per rinvio) al documento informatico con firma digitale non conforme, come ha sostenuto per anni la dottrina anteriore al D.P.R. n. 513/1997. In tal modo, rendendo fin da ora su questo importante punto il T.U. compatibile con la direttiva comunitaria.

Ritenendo, invece, esclusa l'applicabilità dell'art. 2712 c.c. alle firme elettroniche (non avanzate), resta la possibilità di un loro ingresso in giudizio come prove atipiche, liberamente

valutabili, soggette al principio del libero convincimento del giudice (art. 116 c.p.c.). Inoltre, un documento con firma elettronica potrebbe costituire principio di prova per iscritto e, quindi, giustificare una deroga al divieto della prova testimoniale - e per presunzioni (art. 2729 comma 2 c.c.) - che vige per certi contratti (art. 2724 n. 1 c.c.).

2.4 Le forme informatiche

Se per forma si intende il modo in cui avviene la manifestazione di volontà, la documentazione informatica è una nuova forma che viene espressamente introdotta nel nostro ordinamento e si affianca alle forme già esistenti (scritta ed orale). O meglio, la documentazione informatica rappresenta una nuova categoria di forme, dato che sono previste diverse forme di documento informatico (non sottoscritto, sottoscritto con firma digitale conforme al T.U., sottoscritto con firma digitale autenticata da un notaio, sottoscritto con firma elettronica, copia informatica di atto pubblico). Il T.U. ed i successivi provvedimenti di attuazione descrivono e regolano i modelli delle forme informatiche, che assumeranno rilevanza giuridica solo se possiedono tutti i caratteri e requisiti di volta in volta prescritti.

Peraltro, le norme già esistenti sulla forma non sono cambiate, dato che non sarebbe pensabile di riscriverle tutte, inserendovi la previsione della nuova forma informatica. Per questo, il T.U. ha stabilito, in varie norme, un'equiparazione legislativa tra le nuove forme informatiche e le forme già conosciute. In tal modo, le prescrizioni di forma che fanno riferimento alla "sottoscrizione", "scritto", "scrittura privata", "scrittura privata autentica", sono ugualmente soddisfatte dalla creazione di documenti informatici con certi requisiti. Ad es., non è necessario riscrivere l'art. 1350 c.c., che richiede la forma scritta (scrittura privata o atto pubblico) per il compimento di alcuni atti aventi ad oggetto beni immobili, inserendo la previsione della nuova forma informatica, ma quest'ultima sarà ugualmente applicabile in virtù dell'art. 10 T.U. La stessa direttiva CE "non disciplina aspetti relativi alla conclusione e alla validità dei contratti o altri obblighi giuridici quando esistono requisiti relativi alla forma prescritti dal diritto nazionale o comunitario, né pregiudica le norme e i limiti che disciplinano l'uso dei documenti contenuti nel diritto nazionale o comunitario" (art. 1 direttiva); vedi anche considerando n. 17 e n. 21.

Ma, si badi bene, la forma informatica non "è" "sottoscrizione", "scritto", "riproduzione meccanica", "scrittura privata"; bensì "equivale alla sottoscrizione" (art. 23 comma 2 T.U.), "soddisfa il requisito legale della forma scritta" (art. 10 comma 1 T.U.), "ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile" (art. 10 comma 1 T.U.), "ha efficacia di scrittura privata ai sensi dell'art. 2702 c.c." (art. 10 comma 3 T.U.). In altri termini, si riconosce la differenza ontologica tra forme informatiche e forme tradizionali, ma se ne equipara la funzione e l'efficacia probatoria. Non si estendono concettualmente i termini giuridici che fanno riferimento alla "forma scritta" ed alla "scrittura privata", per comprendervi anche la nuova forma informatica, ma se ne stabilisce un'equiparazione. Non è escluso che le norme di prossima emanazione, nel dettare prescrizioni sulla forma, prevederanno direttamente la forma informatica unitamente ad altre forme cartacee, o addirittura in via esclusiva, considerando le garanzie diverse che offre (maggiori o minori per i diversi aspetti).

L'equivalenza tra firma digitale e sottoscrizione (art. 23 comma 2 T.U.), dal punto di vista formale, consente di ritenere soddisfatte con una firma digitale (conforme al T.U.) tutte le prescrizioni di forma che fanno riferimento alla sottoscrizione.

Il documento informatico "redatto in conformità alle regole tecniche" e "sottoscritto con firma digitale" soddisfa "il requisito legale della forma scritta" ed ha "efficacia probatoria ai sensi dell'articolo 2712 c.c." (art. 10 comma 1 T.U.).

La dottrina già da diverso tempo sosteneva che il documento informatico poteva essere considerato un documento scritto a tutti gli effetti. Il regolamento approvato con D.P.R. n.

513/1997 sembrava accogliere questa teorizzazione quando stabiliva nell'art. 4 comma 1, che "Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta". Il regolamento non qualificava espressamente il documento informatico come documento scritto, ma piuttosto disponeva che "soddisfa il requisito legale della forma scritta". Peraltro, la "forma" scritta è correttamente equiparabile non al "documento" informatico ma alla "documentazione" informatica. Dunque, la norma andrebbe letta nel senso che "la documentazione informatica munita dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta". Diversamente, volendo fare riferimento al profilo della prova (e non della forma), e ponendo l'accento sul "documento", la norma andrebbe correttamente riformulata nel senso che "il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della prova scritta".

La dottrina, infatti, distingue la forma (o documentazione) del negozio dalla sua prova (o documento). La prima non è una cosa, ma un'attività; la seconda è una *res*, rappresentazione e prodotto di quest'attività. Quando la forma è richiesta *ad substantiam* (a pena di validità, art. 1325 n. 4 c.c.), rileva non la *res* (la cosa, lo scritto, la carta, il documento), ma l'attività di documentazione che deve accompagnare la dichiarazione. La categoria della cosiddetta forma richiesta *ad probationem* (art. 2725 c.c.) è, invece, logicamente inammissibile: in realtà si intende una più rigorosa disciplina della prova testimoniale e, dunque, non la forma dell'atto, ma bensì la "forma della prova".

Il T.U. anche su questo punto si discosta in modo sostanziale dal D.P.R. n. 513/1997, il quale, ai fini della parificazione con la forma scritta, richiedeva che il documento informatico fosse solo "munito dei requisiti previsti dal presente regolamento" (art. 4 D.P.R. n. 513/1997), senza però precisare cosa si intendesse con tale espressione e senza richiedere espressamente anche la sussistenza di una firma digitale. Peraltro, vigente il D.P.R. n. 513/1997, nonostante la detta formulazione, appariva già alquanto difficile considerare come "scritto" il documento informatico senza firma digitale.

La norma in questione assume un'importanza fondamentale nel sistema del T.U., se messa in relazione alla norma del comma 3 dello stesso art. 10 T.U. Infatti, mentre il comma 3 fa riferimento solo al piano dell'efficacia probatoria del documento già formato, il comma 1 fa riferimento al piano dell'attività formale di documentazione. In tal modo è possibile equiparare il documento informatico con firma digitale alla scrittura privata sul piano della forma (attività), oltre che sul piano della prova (documento, risultato dell'attività), permettendo di compiere in forma informatica gli atti per i quali la forma scritta è richiesta *ad substantiam* (ad es. art. 1350 c.c.). Questa interpretazione sistematica, operata sul piano della forma (e non del documento), consente di assegnare un ruolo all'art. 10 comma 1 T.U., il quale sarebbe, altrimenti, una mera petizione di principio, con effetti alquanto modesti nell'ordinamento civilistico italiano, dato che la norma sarebbe circoscritta ai rari casi in cui è richiesta la prova scritta ma non sottoscritta.

Così ragionando, possono essere stipulati in originale ed in forma esclusivamente informatica, atti giuridici per i quali è richiesta *ad substantiam* la forma minima della scrittura privata (art. 1325 n. 4 c.c.), come ad es. atti aventi ad oggetto beni immobili (art. 1350 c.c.). Gli atti stipulati in forma informatica possono, poi, essere immessi direttamente nei sistemi di pubblicità legale, come i Registri immobiliari (artt. 2656, 2657, 2835, 2836 c.c. che richiedono quale titolo minimo la scrittura privata autenticata o accertata giudizialmente) ed il Registro delle imprese (art. 2189 comma 2 c.c. ed art. 11 D.P.R. 7 dicembre 1995, n. 581, per cui le iscrizioni nel Registro delle imprese sono eseguite previo accertamento dell'autenticità della sottoscrizione), anche mediante trasmissione telematica in via definitiva della richiesta (nota o domanda) e del titolo.

In virtù del principio della libertà della forma, che si ritiene vigente nel nostro ordinamento, in assenza di specifiche prescrizioni di forma, l'atto potrebbe essere liberamente compiuto con una qualsiasi delle forme informatiche.

È escluso che tramite un documento informatico senza firma digitale o con firma elettronica (semplice) possa essere integrato il requisito della forma scritta richiesta *ad substantiam* (ad es. art. 1350 c.c.), o *ad probationem*.

2.5 L'autenticazione di firma digitale

Si è prima chiarito che la verifica tecnica di una firma digitale mediante una chiave pubblica certificata da un certificatore, non fornisce alcuna certezza circa il reale autore della firma stessa, bensì solo sull'identità del soggetto titolare del relativo certificato. Solo un meccanismo di tipo presuntivo, ricollegato all'esclusività di uso del dispositivo di firma, consente di attribuirne la provenienza al suo titolare certificato. Come stabilisce l'art. 23 comma 3 T.U., "La firma digitale deve riferirsi in maniera univoca ad un solo soggetto", ma non è dato sapere se sia effettivamente tale soggetto il reale sottoscrittore.

Nel sistema del T.U., l'unico strumento che fornisce la garanzia della reale identità del sottoscrittore, cioè che la firma digitale sia stata apposta spontaneamente e coscientemente dall'effettivo titolare della chiave certificata e non da altri, consiste nell'autenticazione della firma digitale stessa ai sensi dell'art. 24 T.U. Non sembra possibile l'autenticazione ai sensi dell'art. 24 T.U. di una "firma elettronica" non avanzata.

Seguendo la detta prospettiva di simmetria tra documentazione cartacea ed informatica, riproducendo in parte l'art. 2703 c.c., la struttura dell'autentica è delineata prescrivendo che "l'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza [art. 72 l. not.] dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte [art. 47 comma 3 l. not., art. 67 reg. not.] e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, numero 1°, della legge 16 febbraio 1913, n. 89" (legge notarile). La norma, questa volta non si limita ad operare un mero rinvio (come fa l'art. 10 comma 3 T.U. in relazione all'art. 2702 c.c.), ma detta specifiche disposizioni valide per le firme digitali, risolvendo così in partenza molti dei possibili problemi applicativi.

Il notaio o altro pubblico ufficiale autorizzato (art. 24 comma 1 T.U.), quale soggetto terzo ed imparziale, certifica innanzitutto la reale identità della parte che sottoscrive con firma digitale.

Egli indaga, inoltre, la volontà del sottoscrittore e la traduce in termini giuridici, con lo scopo di produrre un documento che raggiunga efficacemente gli interessi e gli effetti voluti dalle parti, riducendo le possibilità di future contestazioni, nella prospettiva di funzione preventiva ed antigiusdizionale dell'ufficio notarile.

Infine, esegue il controllo di legalità e di conformità all'ordinamento giuridico dell'atto autenticato, producendo documenti che costituiscono titolo per le modifiche dei registri di pubblicità legale, assumendosi la responsabilità nei confronti delle parti della corretta esecuzione di tutti i compiti cui è chiamato. Va notato che per la prima volta è prescritta espressamente da una norma l'esecuzione del controllo di legalità da parte del notaio (art. 28 legge notarile), chiamato ad operare un'autenticazione di un documento avente efficacia di scrittura privata, confermando precedenti e consolidati orientamenti giurisprudenziali in tal senso.

La firma digitale da autenticare deve essere apposta dal titolare della chiave, il che significa, evidentemente, che dovrà essere lui stesso ad azionare l'*hardware* ed il *software* per il calcolo della firma digitale. Non saranno richieste particolari competenze informatiche, dato che si tratterà di semplici operazioni (come ad es. lettura nello schermo del *computer*,

inserimento di una *smart card*, digitazione di un *pin* o esibizione di una parte del corpo per il riconoscimento biometrico), per le quali il notaio potrà dare la sua assistenza, senza togliere nulla al carattere “personale” della firma. Non è concepibile, allo stato attuale un’autentica a distanza, essendo richiesta la presenza del firmatario davanti il notaio. Tuttavia, come già vale per la documentazione cartacea, sarà ammissibile che un contratto in forma informatica rechi sottoscrizioni autenticate da notai diversi ed in luoghi diversi, che vengono, poi, trasmesse, anche in via telematica.

Il notaio o altro pubblico ufficiale sottoscrive l’autentica apponendo la propria firma digitale (art. 24 comma 3 T.U.), la quale sostituisce “la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti” (anche art. 23 comma 6 T.U.). Quest’ultima disposizione, la cui portata deriva comunque dalle intrinseche caratteristiche della documentazione informatica, autorizza l’omissione del sigillo notarile *ex art. 52 l. not.*, richiesto anche nell’autenticazione di scrittura privata dall’art. 72 l. not.

Evidentemente, l’apposizione della firma digitale da parte del notaio è un atto strettamente personale, che comporta l’attivazione del dispositivo di firma da parte del titolare e non di altri, eventualmente subordinata al personale riconoscimento biometrico.

La provenienza da parte di un pubblico ufficiale, consente di inquadrare la autenticazione *ex art. 24 T.U.* nel novero degli atti pubblici. L’autentica attribuisce, inoltre, data certa (art. 2704 c.c.) al documento informatico autenticato.

La verifica dell’autentica notarile si effettua mediante la chiave pubblica del notaio, con un certificato che ne attesta anche la sussistenza della qualifica e dei pubblici poteri.

L’efficacia probatoria della scrittura privata informatica autenticata è quella stessa stabilità per la sottoscrizione autenticata su carta dall’art. 2703 c.c. La disposizione dell’art. 24 comma 1 T.U., riproduce in modo sostanzialmente identico il contenuto dell’art. 2703 c.c., e nello stesso tempo vi rinvia espressamente. La firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato “si ha per riconosciuta” (art. 24 comma 1 T.U. ed art. 2703 comma 1 c.c.) e, pertanto, ai sensi dell’art. 2702 c.c., farà piena prova della provenienza delle dichiarazioni da chi ha sottoscritto il documento informatico, anche se colui contro il quale è prodotto non riconosce la sottoscrizione, salvo l’esperibilità della querela di falso.

Il fatto che la firma digitale autenticata si consideri di per sé come “riconosciuta”, comporta che non occorra l’esperimento del formale giudizio di verifica affinché essa acquisisca piena prova e che, pertanto, non possa essere direttamente disconosciuta ma solo contestata con un procedimento di querela di falso. In presenza di un’autenticazione *ex art. 24 T.U.*, l’ipotesi che la firma sia stata apposta da un soggetto diverso dal titolare della chiave, può essere fatta valere solo con la querela di falso, costituendo un falso ideologico. Allo stesso modo, può essere fatta valere la falsità della firma digitale del pubblico ufficiale autenticante (falso materiale), nei casi in cui la carta (dispositivo di firma) sia stata concretamente utilizzata da persona diversa dal notaio (ad es. la sua segretaria).

La possibilità di ottenere un’autenticazione di firma digitale, rappresenta un’opportunità aggiuntiva e non certo un appesantimento del nuovo traffico giuridico in forma informatica. Le parti sono libere di produrre documenti giuridici ed apporre firme digitali o elettroniche senza richiedere l’intervento notarile. Nulla è innovato nel regime giuridico delle prescrizioni di forma che richiedono la sottoscrizione autenticata. Peraltro, l’autentica potrà essere liberamente richiesta al notaio nei casi in cui le garanzie che essa offre si reputano opportune e convenienti in relazione agli interessi in gioco; l’autentica sarà, invece, obbligatoria solo nelle ipotesi in cui oggi è già richiesto l’intervento notarile, come ad es. per i documenti da immettere nei registri di pubblicità legale. Anche la direttiva CE è ispirata al principio che “le disposizioni sugli effetti giuridici delle firme elettroniche non dovrebbero pregiudicare i

requisiti formali previsti dal diritto nazionale sulla conclusione dei contratti” (considerando n. 17 direttiva CE).

Il T.U. non prevede, ma nemmeno esclude, la redazione di un atto pubblico notarile originale in forma informatica. Tuttavia, anche a voler oggi negare tale possibilità, in considerazione delle stringenti prescrizioni formali della legge notarile (legge 16 febbraio 1913, n. 89), il T.U. prevede la copia informatica di un atto pubblico redatto originariamente su carta, che offre, comunque, già di per sé vastissime prospettive di applicazione pratica. Ad es. sarà possibile trasmettere telematicamente un atto pubblico, mantenendone la fede privilegiata, previa effettuazione di una copia informatica (un notaio potrebbe ricevere telematicamente da un altro notaio una procura speciale da allegare all’atto pubblico ai sensi dell’art. 51, n. 3 l. not.); e con tali copie in forma informatica si potranno, richiedere modificazioni nei registri di pubblicità legale (in particolare Registri immobiliari e Registro delle imprese); inoltre, dalla copia informatica di un atto pubblico si potranno ricavare duplicati con piena efficacia probatoria, senza che necessiti un nuovo intervento del notaio depositario dell’originale cartaceo, non potendosi – allo stato dell’attuale tecnologia – limitarne facilmente l’ulteriore duplicabilità in modo controllabile.

Il D.LGS. 18 gennaio 2000, n. 9, aggiungendo al D.LGS. 18 dicembre 1997, n. 463 l’art. 3 *bis*, prevede che “Alla registrazione di atti relativi a diritti sugli immobili, alla trascrizione, all’iscrizione e all’annotazione nei registri immobiliari, nonché alla voltura catastale, si provvede, a decorrere dal 30 giugno 2000, con procedure telematiche”, mediante la trasmissione di un “modello unico informatico”, che comprende le formalità della richiesta di registrazione, la nota di trascrizione e di iscrizione nonché le domande di annotazione e di voltura catastale.

Il D.P.R. 18 agosto 2000, n. 308 (Regolamento concernente l’utilizzazione di procedure telematiche per gli adempimenti tributari in materia di atti immobiliari) distingue tra atti le cui copie sono in forma informatica con firma digitale conforme al D.P.R. n. 513/1997 (art. 1) ed atti non implicanti l’impiego della firma digitale (art. 2). Per i primi, occorrerà trasmettere il modello unico informatico, unitamente a copia dell’atto (autenticata con firma digitale). Per i secondi, successivamente alla trasmissione telematica del modello unico informatico e di copia (informatica) dell’atto, occorrerà la presentazione del titolo in forma cartacea per l’esecuzione delle formalità ipotecarie, con la restituzione del duplo cartaceo della nota (art. 6); ai fini della registrazione fiscale non è più richiesta la presentazione dell’atto originale, in quanto si prevede che “la documentazione in originale è conservata dal pubblico ufficiale” (art. 2 comma 2; vedi anche l’art. 36 della legge n. 340/2000), mentre l’Amministrazione finanziaria rende disponibile una ricevuta per via telematica e può chiedere “l’esibizione della documentazione relativa agli atti trasmessi per via telematica, ovvero di esaminare la stessa presso la sede del pubblico ufficiale” (art. 2 comma 6). In entrambi i casi la voltura catastale è eseguita automaticamente a seguito della presentazione del modello unico informatico e gli uffici dell’Amministrazione finanziaria rendono disponibile per via telematica l’attestazione di eseguita voltura (art. 5). Il decreto ministero finanze 13 dicembre 2000 (G.U. n. 302 del 29 dicembre 2000) reca l’approvazione del modello unico informatico e delle modalità tecniche necessarie per la trasmissione dei dati. La circolare del Ministero delle finanze – Agenzia delle entrate del 29 marzo 2001, n. 33/E disciplina la fase sperimentale dell’attivazione del servizio telematico.

Molto correttamente, le disposizioni riportate fanno riferimento ad un tipo di documentazione informatica conforme all’impianto normativo italiano della firma digitale, richiamando l’osservanza del D.P.R. n. 513/1997 (ora T.U.). È escluso, pertanto, che un documento con firma digitale non conforme al D.P.R. n. 513/1997 (ora T.U.) ed alle relative regole tecniche, possa costituire titolo idoneo per l’iscrizione o deposito nei registri immobiliari (o in altri registri di pubblicità legale), tutte le volte in cui è richiesta la

produzione di un documento autentico. Pertanto, insieme alla trasmissione di documenti con firma digitale non conforme, è necessaria ed ineliminabile la produzione dei relativi documenti cartacei autentici.

Identico ragionamento è valido per gli atti che i notai trasmettono al Registro delle imprese - in quanto registro di pubblicità legale con effetti di opponibilità nei confronti dei terzi (art. 2193 c.c.) – i quali devono essere “autentici” in senso lato, cioè muniti di una sottoscrizione autenticata o di una dichiarazione di conformità in caso di copie (ad es. art. 2189 c.c., art. 11 D.P.R. n. 581/1995, art. 2206 c.c., art. 2296 c.c., art. 2330 c.c., art. 2479 c.c., art. 2556 c.c.). L’art. 4 comma 1 del D.P.R. n. 558/1999 (Regolamento recante norme per la semplificazione della disciplina in materia di registro delle imprese), prevede che “Decorso un anno dalla data di entrata in vigore del presente regolamento [entra in vigore il 6 dicembre 2000] tutte le domande di iscrizione e di deposito e gli atti che le accompagnano presentate all’ufficio del registro delle imprese, ad esclusione di quelle presentate dagli imprenditori individuali, sono inviate per via telematica ovvero presentate su supporto informatico. Le modalità e i tempi per l’assoggettamento al predetto obbligo degli imprenditori individuali sono stabilite con regolamento del Ministro dell’industria, *tenuto conto della normativa di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513 [ora T.U. 445/2000]*” (il corsivo è mio). Tale norma è riproposta in modo simile nell’art. 31 comma 2 della legge n. 340/2000 (Legge di semplificazione 1999), secondo cui “Decorso un anno dalla data di entrata in vigore della presente legge [entra in vigore il 9 dicembre 2000], le domande, le denunce e gli atti che le accompagnano presentate all’ufficio del registro delle imprese, ad esclusione di quelle presentate dagli imprenditori individuali e dai soggetti iscritti nel repertorio delle notizie economiche e amministrative di cui all’articolo 9 del decreto del Presidente della Repubblica 7 dicembre 1995, n. 581, sono inviate per via telematica ovvero presentate su supporto informatico *ai sensi dell’articolo 15, comma 2, della legge 15 marzo 1997, n. 59*. Le modalità ed i tempi per l’assoggettamento al predetto obbligo degli imprenditori individuali e dei soggetti iscritti solo nel repertorio delle notizie economiche e amministrative sono stabilite con decreto del Ministro dell’industria, del commercio e dell’artigianato” (il corsivo è mio). Anche tali norme, correttamente fanno riferimento al D.P.R. n. 513/1997 ed alla legge n. 59/1997. È escluso, pertanto, che un documento con firma digitale non conforme al D.P.R. n. 513/1997 (ora T.U.) ed alle relative regole tecniche, possa costituire titolo idoneo per l’iscrizione o deposito nel registro delle imprese (o in altri registri di pubblicità legale), tutte le volte in cui è richiesta la produzione di un documento autentico. Né potrebbe costituire titolo idoneo un documento informatico con firma elettronica (semplice) ai sensi della direttiva comunitaria, dato che le garanzie proprie della firma elettronica avanzata (espresse nell’art. 2 della direttiva CE), sono imprescindibile fondamento di un sistema di pubblicità legale.

La circolare del ministero delle attività produttive n. 3529/C del 30 ottobre 2001 avente ad oggetto l’attuazione del sopra citato art. 31 della legge n. 340/2000, prende atto degli “impedimenti obiettivi” che non consentono la piena applicazione del detto disposto e consente che le pratiche al registro delle imprese potranno essere presentate non solo per via telematica con firma digitale, ma anche presentando allo sportello il *floppy* con il software FEDRA (anche senza firma digitale). In ogni caso, se non è utilizzata la firma digitale conforme (che è facoltativa), è richiesta la presentazione delle copie autentiche degli atti in forma cartacea. In definitiva, rispetto al passato, dal 9 dicembre 2001 non sarà più accettata la modulistica cartacea.

La convenzione sottoscritta il 25 ottobre 2001 tra il Consiglio Nazionale del Notariato, Unioncamere, Infocamere e Notartel s.p.a., valida fino alla completa attuazione della firma digitale a norma, prevede che per la trasmissione telematiche delle pratiche al registro delle imprese i notai possano utilizzare firme digitali generate con un dispositivo di firma rilasciato

da Infocamere, fermo restando l'obbligo di presentare entro cinque giorni dall'invio telematico la pratica cartacea completa di tutti gli atti e documenti già inviati telematicamente (ed in particolare la copia autentica dell'atto depositato). Nel momento in cui i notai potranno apporre firme digitali pienamente conformi alla legge ed in particolare a norma del citato art. 29 comma 3 T.U. (certificazione autonoma e con il controllo della funzione), le copie informatiche potranno sostituire agevolmente le copie su carta, in virtù dell'efficacia loro riconosciuta ai sensi dell'art. 20 come appresso esaminato.

2.6 Le copie informatiche

Le innumerevoli - ed ancora inimmaginabili applicazioni e vantaggi dei documenti informatici - derivano fondamentalmente dal fatto che si verifica un completo distacco del contenuto dal contenente. In un documento si distingue tra elemento materiale (il supporto-contenente) ed elemento spirituale o intellettuale (il suo contenuto); il primo è il mezzo nel quale è incorporata la scritturazione, ossia i segni alfabetici che compongono il pensiero; il secondo è il pensiero espresso materializzato nello scritto.

Nel documento cartaceo, l'elemento spirituale non avrebbe alcun valore se distaccato dall'elemento materiale. Tanto l'integrità, quanto l'imputabilità fondano la loro garanzia sul collegamento col supporto: la sottoscrizione, in quanto tale, svolge le sue funzioni solo perché legata indissolubilmente al supporto materiale, ed è sicura in quanto non è da questo staccabile né alterabile. Da ciò consegue che al supporto è, in ultima analisi, affidata non solo l'integrità del contenuto, ma anche la garanzia della provenienza: di guisa che nel tradizionale modo di intendere il documento assistiamo ad un'assoluta preminenza dell'elemento materiale (il contenente) rispetto all'elemento spirituale (il contenuto), il quale di per sé considerato sarebbe privo di qualunque efficacia probatoria. In ragione di questo legame tra contenente e contenuto deriva l'esigenza dell'intervento di un notaio o altro pubblico ufficiale (artt. 2714-2719 c.c.), indispensabile per garantire l'integrità della copia di un atto nel momento del trasferimento dal contenente (originale) al contenente (copia), e quindi per conservarne l'efficacia probatoria.

Con le firme elettroniche si ribalta il rapporto tra supporto e contenuto del documento. La sicurezza del documento informatico con firma elettronica, cioè la possibilità di accertarne integrità e provenienza, non risiede più nel supporto materiale (contenente), ma unicamente nell'elemento intellettuale, cioè nel contenuto del documento stesso. In termini informatici, una sicurezza giuridica ed un'autenticazione basata solo su strumenti *software* e non *hardware*.

Non ci sono più ostacoli alla creazione di documenti del tutto immateriali, duplicabili e trasmissibili senza che perdano il loro valore; con un contenuto completamente svincolato dal contenente; un contenuto che è libero di passare da un contenente ad un altro mantenendo tutte le sue garanzie di autenticità e di efficacia probatoria, con un'assoluta mobilità del documento. A tal proposito, con un'efficace espressione, si è parlato di "passaggio dagli atomi ai bits" (NEGROPONTE).

Essendo la "copia" informatica di un documento informatico indistinguibile dal suo "originale" (la "copia" di un *bit* è uguale al *bit* "originale"), non ha più alcun senso una distinzione tra "originale" e "copia" di un documento informatico: al termine "copia" è allora preferibile il termine "duplicato". Questa caratteristica della documentazione informatica, per la quale non è applicabile il concetto di "possesso" materiale, la rende, tra l'altro, inidonea alla rappresentazione di documenti destinati a circolare in singoli esemplari originali (come ad es. i titoli di credito), a meno che non si implementi un registro centralizzato (*on-line*) per il monitoraggio della circolazione del documento e delle persone legittimate ad esibirlo o si utilizzi dell'*hardware* a prova di falsificazioni; allo stesso modo di quanto sarebbe necessario

per limitare la duplicabilità dei documenti informatici aventi efficacia di scrittura privata o (copia di) atto pubblico, come si è prima detto.

Su questo presupposto tecnico fondamentale, il T.U., riconoscendo il non senso della distinzione tra originale e copia di un documento informatico, stabilisce che “I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi alle disposizioni del presente testo unico” (art. 20 comma 1 T.U.).

A tal fine, non occorre l'intervento di un notaio o altro pubblico ufficiale a garanzia della conformità del contenuto del duplicato, dato che non si pone alcun problema di conformità della “copia” all'originale”. Qualunque difformità tra “copia” ed “originale”, risultando non più in un duplicato, porterebbe di per sé ad una mancata verificabilità delle firme elettroniche (semplici o avanzate) eventualmente apposte.

Pertanto, il documento informatico con firma elettronica può essere duplicato da chiunque, e senza limiti nel numero dei duplicati, mantenendo sempre la stessa identica efficacia probatoria, senza che possa parlarsi di copia di copia (art. 2714 comma 2 c.c.). Il documento informatico con firma digitale autenticata ex art. 24 T.U., se conservato a raccolta negli atti del notaio ex art. 61 l. not., sarà duplicato in prima istanza dal notaio depositario, e successivamente potrà essere liberamente duplicato dalle parti o da chiunque ne sia venuto in possesso.

Se un documento informatico con firma digitale viene duplicato, omettendone delle parti, oppure omettendo la firma stessa, non si otterrà più un duplicato, bensì un documento diverso che non avrà la stessa efficacia probatoria. Così, l'estratto (o copia parziale) di un documento informatico, non potendo tecnicamente essere verificato con la firma digitale apposta al documento integrale, dovrà contenere una dichiarazione di conformità da parte del pubblico ufficiale, con una sua firma digitale riferita al nuovo contenuto estratto. L'efficacia probatoria dell'estratto informatico sarà quella stessa prevista dall'art. 2718 c.c.

Le copie informatiche di documenti cartacei sono disciplinate dall'art. 20 comma 3 T.U., che parla di “copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico”.

A differenza del duplicato, sopra esaminato, tali copie “sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte [solo] se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato” (art. 20 comma 3 T.U.).

L'intervento autenticante del pubblico ufficiale è, in questo caso, indispensabile per conservare l'efficacia probatoria del documento, a garanzia dell'integrità e conformità del suo contenuto, nel passaggio dal contenente-supporto carta (o altro non informatico) al supporto informatico, in modo analogo a quanto è richiesto per le tradizionali copie cartacee nel passaggio da un foglio ad un altro (artt. 2714 ss. c.c.; art. 69 comma 2 l. not.; art. 18 T.U.). L'autentica dovrebbe essere richiesta anche per gli estratti (o copie parziali) informatici di documenti cartacei (art. 2718 c.c.).

L'autentica da parte del pubblico ufficiale dovrà consistere in una “dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3” (art. 20 comma 3 T.U.). Le regole tecniche emanate con d.p.c.m. 13 febbraio 1999 non prevedono però ancora le modalità per l'effettuazione di copie informatiche di documenti non informatici a cui rinvia l'art. 20 comma 3 T.U. Tuttavia, sarà evidentemente indispensabile, l'apposizione della firma digitale del pubblico ufficiale, così come è previsto per la particolare e più specifica ipotesi del comma 2 dello stesso articolo. E dovrà trattarsi di una firma digitale pienamente a norma, certificata nel rispetto delle prescrizioni di cui al citato art. 29 comma 3 T.U. (certificazione autonoma e con il controllo della funzione).

Le copie informatiche di documenti cartacei, autenticate ai sensi dell'art. 20 comma 3 T.U., possono essere allegate ad un documento informatico autenticato (art. 24 comma 4 T.U.).

La disposizione dell'art. 20 comma 2 T.U. specifica ulteriormente l'efficacia delle copie informatiche, attribuendogli "piena efficacia ai sensi degli artt. 2714 e 2715 del codice civile, se ad esse è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente testo unico".

La citata norma dell'art. 20 comma 2 T.U., pur non precisandolo espressamente, non può che riferirsi ed assumere significato in relazione all'ipotesi delle copie informatiche di originali cartacei. Come si è già detto, non avrebbe, infatti, alcun senso richiedere un'autenticazione per il rilascio di un duplicato di un documento informatico. Tale ricostruzione è confermata dal successivo comma 4 dello stesso art. 20 T.U., per il quale le copie rilasciate *ex art. 20 comma 2 T.U.* possono essere prodotte ed esibite in luogo dell'"originale formato su supporto cartaceo", con ciò presupponendo l'effettuazione di una copia da carta a supporto informatico. Peraltro, l'esenzione dalla produzione e dall'esibizione dell'originale cartaceo è già chiaramente desumibile dall'art. 20 comma 3 T.U., che stabilisce la sostituzione ad ogni effetto di legge delle copie informatiche agli originali cartacei.

Le copie informatiche di documenti cartacei (atti pubblici o scritture private) potranno poi essere ulteriormente duplicate da chiunque senza necessità di alcuna autenticazione, in base al principio prima chiarito. Non si tratta, infatti, di copie di copie (art. 2714 comma 2 c.c.), ma di duplicati di documenti informatici, che rientrano nella disciplina dell'art. 20 comma 1 T.U. sopra esaminata, e come tali indistinguibili dalla prima copia rilasciata dal pubblico ufficiale, salvo le condizioni prima indicate (registro centralizzato o *hardware* specifico).

Non è disciplinato il passaggio inverso, dal supporto informatico al supporto non informatico (carta o altro), cioè l'effettuazione di copie cartacee di documenti informatici.

Identità di *ratio*, porterebbe all'applicazione analogica dell'art. 20 commi 3 e 2 T.U. e dell'art. 2719 c.c., richiedendo l'intervento del pubblico ufficiale che attesti la conformità della copia su carta. A conferma di questa interpretazione si richiamano le regole tecniche per l'uso dei supporti ottici (deliberazione AIPA n. 24/1998), le quali prevedono all'art. 6 comma 4 (simmetricamente all'art. 11 dello stesso provvedimento) che per l'esibizione su supporto cartaceo di documenti contenuti in supporto ottico è necessaria l'autenticazione di un pubblico ufficiale.

In conclusione, ad esclusione delle copie tra supporti diversi (informatici e cartacei, in un senso o nell'altro), non occorre l'intervento del pubblico ufficiale, ed assume una piena valenza la disposizione dell'art. 20 comma 1 T.U., per il quale "i duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge".

3 LA VALIDAZIONE TEMPORALE

3.1 La validazione temporale

La stessa tecnologia della cifratura asimmetrica consente l'apposizione di marche temporali (*digital time stamp*) che attestano la data e l'ora di un *file* informatico, con l'intervento ancora una volta imprescindibile di una terza parte fidata. Dal punto di vista tecnico, la validazione temporale consiste essenzialmente nei seguenti passaggi:

- 1) Tizio applica al *file* M una funzione di *hash* ed ottiene l'impronta M_D ;
- 2) Tizio invia (telematicamente) l'impronta M_D al servizio di validazione temporale;

3) il servizio di validazione temporale aggiunge la data e l'ora ad M_D , ed applicando all'insieme la propria chiave privata K_S , con un algoritmo di cifratura asimmetrico, calcola la marca temporale T ;

4) la marca temporale T è spedita (telematicamente) a Tizio che la allega al documento M .

La verifica della autenticità della data ed ora apposta si ottiene applicando la corrispondente chiave pubblica K_P del servizio di validazione temporale, alla marca temporale e confrontando il risultato con l'impronta M_D (ricalcolata) del *file* M , in modo analogo alla verifica di una firma digitale.

Secondo il T.U., si intende “per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi” (art. 2 comma 1 lett. g). Si intende, per “marca temporale”, un'evidenza informatica che consente la validazione temporale” (art. 1 lett. f reg. tec.).

Le marche temporali sono generate da un apposito “sistema elettronico sicuro” (art. 52 comma 2, art. 11 comma 5 lett. b ed art. 54 comma 1 reg. tec.), gestito dagli stessi certificatori, che stabiliscono, pubblicandole nel manuale operativo, le procedure per l'inoltro della richiesta (art. 58 comma 1 reg. tec.). La richiesta deve contenere l'evidenza informatica (il *file*) nella sua interezza - oppure alternativamente la sua impronta - alla quale la marca temporale deve essere riferita. L'invio della sola impronta consente di non svelare il contenuto dell'evidenza informatica (ad es. un'opera dell'ingegno).

La generazione (e la verifica) della marca temporale avviene applicando una specifica chiave di marcatura temporale (art. 4 comma 4 lett. c reg. tec.). La generazione delle chiavi di marcatura temporale può essere effettuata esclusivamente dal responsabile del servizio che utilizzerà le chiavi (art. 6 comma 1 reg. tec.). Le chiavi di marcatura temporale sono anch'esse certificate dal certificatore, mediante associazione univoca ad un sistema di validazione temporale (art. 54 comma 1 reg. tec.), e nel relativo certificato (in aggiunta a quanto già previsto per le altre tipologie di chiavi) devono essere indicati: a) l'uso delle chiavi per la marcatura temporale; b) l'identificativo del sistema di marcatura temporale che utilizza le chiavi (art. 11 comma 5 reg. tec.). I certificati delle chiavi di marcatura temporale vanno, in ogni caso, sottoscritti con “chiavi di certificazione diverse da quelle utilizzate per i certificati relativi alle normali chiavi di sottoscrizione” (art. 54 comma 3 reg. tec.). In tal modo, la compromissione della chiave di certificazione non compromette anche la marca temporale, e viceversa. Di conseguenza, diventa possibile mantenere la validità del certificato (della chiave di sottoscrizione) a seguito di revoca dei certificati relativi a chiavi di certificazione (art. 38 comma 4 reg. tec.). La marca temporale attesta, infatti, la pubblicazione del certificato in un momento anteriore alla revoca della chiave di certificazione.

In aggiunta, ma non in alternativa, alla validazione temporale, è prevista, dietro richiesta del soggetto interessato, la conservazione di copia del documento informatico cui la marca temporale si riferisce, da parte del certificatore, con modalità di conservazione e procedure per la richiesta del servizio stabilite dal manuale operativo. Questa conservazione andrebbe effettuata “Al solo fine di assicurare l'associazione tra documento informatico e le relative marche temporali” (art. 59 comma 1 reg. tec.). Il certificatore svolge così un servizio analogo alla registrazione degli atti svolta dagli Uffici del registro (art. 2704 c.c.; art. 18 D.P.R. 26 aprile 1986, n. 131). Per dare un senso a tale norma, sembrerebbe, dunque, che adottando questa procedura, anche in caso di scadenza - o altra causa di perdita di validità - della marca temporale, possa in tal modo mantenersi l'efficacia della data ed ora certa opponibile ai terzi (art. 22 comma 1 lett. g T.U.). Mentre, pare che non sarebbe possibile richiedere la conservazione del documento privo di una marca temporale.

L'apposizione di un timbro (validazione) temporale produce l'effetto giuridico di attribuire “ad uno o più documenti informatici una data ed un orario opponibili ai terzi” (art.

22 comma 1 lett. g T.U.) e, dunque, non solo efficaci tra le parti. Una qualche perplessità deriva dal fatto che un tale effetto di opponibilità nei confronti dei terzi non deriva da una qualifica di pubblico ufficiale del servizio di timbratura temporale (i certificatori sono delle s.p.a.). Mentre l'art. 2704 c.c., e le esemplificazioni giurisprudenziali, quando si affidano all'intervento di un terzo, presuppongono, solitamente, la sua qualifica pubblica (così per il notaio, l'ufficio del registro, l'ufficio postale che appone il timbro postale, l'ufficiale giudiziario che effettua un pignoramento, ecc.).

L'apposizione di una marca temporale consente il mantenimento nel tempo della validità e rilevanza della documentazione informatica, a seguito della perdita di validità della chiave per scadenza, revoca o sospensione. Infatti, mentre una sottoscrizione su carta, con il trascorrere del tempo, mantiene in via di principio lo stesso valore probatorio; una firma digitale, invece, è fin dall'inizio destinata a perdere sicurezza in breve tempo per scadenza (predeterminata) a causa dell'inarrestabile progresso nella potenza di calcolo degli elaboratori (il termine di scadenza della chiave non può essere superiore a 3 anni, art. 22 comma 1 lett. f T.U.) o per eventuale revoca o sospensione.

Se la chiave pubblica perde di validità (per scadenza, revoca o sospensione), ne deriva anche una perdita di validità delle firme digitali verificabili con la stessa chiave. A meno che, non si possa dimostrare l'antioriorità della apposizione della firma stessa rispetto alla perdita di validità della relativa chiave (apposizione durante l'*operational period*). Infatti, in mancanza di tale prova, non potrebbe essere escluso il rischio che il documento sia stato falsificato o sottoscritto da un usurpatore (perché ha decifrato chiavi non più sicure o si è impossessato di chiavi altrui); né, possono essere esclusi comportamenti fraudolenti di revoca della chiave (da parte dello stesso titolare), finalizzati al ripudio di precedenti firme digitali.

Se perde validità la firma, viene meno l'efficacia di scrittura privata del documento informatico *ex art. 2702* (art. 10 T.U.). Se perde validità la firma digitale del pubblico ufficiale autenticante *ex art. 24 T.U.*, il documento degrada alla efficacia di scrittura privata non autenticata, purché siano ancora valide le firme digitali delle parti.

Per il mantenimento dell'efficacia di scrittura privata e più in generale per il mantenimento degli effetti giuridici dei documenti connessi alla sussistenza di una sottoscrizione, non sarebbe conclusivo procedere ad una semplice archiviazione del documento (senza marcatura temporale, anche se con le altre più idonee garanzie di conservazione). La perdita di validità della firma impedirebbe qualunque riscontro in sede di disconoscimento, escludendo ogni ipotesi di verifica.

La prova del momento concreto di apposizione della firma digitale, può, ancora una volta, essere fornita solo con l'intervento di un terzo garante, attraverso diverse possibili modalità.

In primo luogo, attraverso una validazione temporale (art. 22 comma 1 lett. g T.U.) della firma digitale. In tal senso, secondo le regole tecniche, con riferimento alla scadenza, "la validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una o più marche temporali" (art. 60 comma 1); con riferimento alla revoca o sospensione, "la presenza di una marca temporale valida associata ad un documento informatico secondo quanto previsto dal comma 2, garantisce la validità del documento anche in caso di compromissione della chiave di sottoscrizione, purché la marca temporale sia stata generata antecedentemente a tale evento" (art. 60 comma 3). *A contrario*, si deduce che in mancanza di una marca temporale, la validità del documento non è garantita, né a seguito di scadenza, né di revoca o sospensione della chiave.

Si tratta, in sostanza di confrontare la marca temporale che attesta il momento di pubblicazione della revoca e della sospensione (artt. 29 comma 3 e 33 comma 2 reg. tec.), con la marca temporale apposta alla firma digitale; nonché quest'ultima marca temporale, con il momento della scadenza della chiave certificata (indicato nel certificato stesso).

La stessa marca temporale, a sua volta, è soggetta a perdita di validità per scadenza. Occorre, dunque, una sua rinnovazione periodica, prima della scadenza, per mantenerne l'efficacia e, correlativamente, mantenere l'efficacia probatoria della firma digitale cui si riferisce (art. 60 reg. tec.). Secondo le regole tecniche, "Prima della scadenza della marca temporale, il periodo di validità può essere ulteriormente esteso associando una nuova marca all'evidenza informatica costituita dal documento iniziale, dalla relativa firma e dalle marche temporali già ad esso associate" (art. 60 comma 2).

Rinnovazione della marca temporale non significa rinnovazione del contratto o del rapporto giuridico documentato. Per cui, se il rapporto termina prima della scadenza della marca temporale rinnovata, non si determina una sua estensione di durata. La rinnovazione della marca temporale serve solo a mantenere l'efficacia probatoria del documento fino alla scadenza del contratto e successivamente.

L'efficacia probatoria dei documenti con autentica notarile *ex art. 24 T.U.* (in quanto aventi data certa) è di per sé mantenuta almeno fino al momento in cui resta validità la firma del notaio, salvo possibilità di prolungare anche la validità di quest'ultima con una validazione temporale o con deposito presso un garante.

In secondo luogo, la prova del momento di apposizione della firma potrebbe realizzarsi mediante affidamento - prima della perdita di validità della chiave - dei documenti informatici (non solo dei loro *hash*) ad un terzo garante che li custodisce, assicurando che non vengano alterati, e li consegna ai legittimati a riceverli, con l'apposizione eventualmente della proprio *attuale* firma digitale a garanzia dell'autenticità. Le regole tecniche, a tal proposito, stabiliscono, che «Al solo fine di assicurare l'associazione tra documento informatico e le relative marche temporali, il certificatore può conservare, dietro richiesta del soggetto interessato, copia del documento informatico cui la marca temporale si riferisce»; «Nel manuale operativo debbono essere definite le modalità di conservazione e le procedure per la richiesta del servizio» (art. 59 commi 1 e 2).

La disposizione che stabilisce il principio di non retroattività della revoca (art. 22 comma 1 lett. 1 T.U.) va, quindi, intesa in senso relativo, cioè che la revoca non travolge le firme digitali anteriormente apposte, a condizione che si possa dimostrare la loro anteriorità temporale rispetto alla decorrenza degli effetti della revoca medesima, o in altri termini possa essere provata l'apposizione durante *l'operational period*, cioè il periodo di validità del certificato.

Nonostante, i rischi sopra rilevati, il regolamento, e le regole tecniche, non stabiliscono l'obbligatoria apposizione di una marca temporale (e la sua rinnovazione) o la necessità di un'autentica *ex art. 24 T.U.* Nemmeno si prevede come obbligatoria la marcatura temporale della firma digitale del notaio autenticante *ex art. 24 T.U.* Si tratta, quindi, di un onere (in senso tecnico) a carico degli interessati che intendono tutelarsi - anche in relazione all'ammontare dei possibili danni - contro la scadenza della chiave o contro eventuali e future revoche. La validazione temporale, unitamente alla firma digitale è, invece, richiesta per la presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione (art. 24 comma 6 T.U.).

In ogni caso, il rinnovo delle marche temporali per preservare l'efficacia giuridica dei documenti implica delle operazioni del tutto algoritmizzabili, che possono essere eseguite da appositi programmi a scadenze programmate in modo automatico e trasparente per l'utente.

Infine, una marca temporale in rinnovazione può essere apposte in un solo momento anche ad un insieme composto da molteplici documenti firmati (ad es. un intero archivio o parte di esso). Tuttavia, in tal caso, la sua verifica comporta che venga preso come parametro (per il calcolo dell'impronta) l'intero archivio (o la sua parte) oggetto della marcatura e non solo il singolo documento in questione.

3.2 Il documento informatico trasmesso telematicamente

La firma digitale apposta ad un documento informatico consente di ottenere il risultato del cosiddetto non ripudio da parte dell'origine: anche se il documento è trasmesso telematicamente, il suo autore (quale risulta dal certificato) non potrebbe negarne con successo la provenienza (se non alle condizioni prima indicate).

Un ulteriore problema è il non ripudio da parte del destinatario di un documento informatico trasmesso telematicamente in una rete aperta come Internet. La soluzione è, tra l'altro, essenziale alla disciplina dei contratti conclusi telematicamente.

Per preconstituire una prova della ricezione di un messaggio telematico, il protocollo più semplice consiste nella restituzione di una ricevuta di ritorno del messaggio, sottoscritta con la chiave privata del destinatario. Ad es. il già citato d.p.r. 18 agosto 2000, n. 308, recante il regolamento sulla trasmissione telematica degli atti in relazione all'adempimento del modello unico informatico, stabilisce che "gli uffici dell'Amministrazione finanziaria rendono disponibile, per via telematica, una ricevuta" (art. 3 comma 3). Il problema di un protocollo di tale specie è che il destinatario spesso non ha alcun interesse a restituire una ricevuta di ritorno, quando dalla ricezione di un atto possono derivare conseguenze sfavorevoli. Si pensi ad es. ad una diffida ad adempiere (art. 1454 c.c.), dalla cui ricezione deriva la decorrenza di un termine per la risoluzione di diritto di un contratto. Occorre, quindi, un sistema che consenta al mittente di preconstituirsì una prova della spedizione e della ricezione del documento informatico da parte del destinatario, senza la necessità della sua collaborazione ed al di fuori del suo controllo.

Ancora una volta non si può prescindere dall'intervento di una terza parte fidata e dal ricorso a delle presunzioni. La terza parte fidata dovrà intervenire per accertare che il documento sia stato effettivamente recapitato e messo a disposizione presso il destinatario in una casella di posta elettronica (*electronic mailbox*) da lui previamente dichiarata, e solo in tal caso emettere una certificazione in tal senso da consegnare al mittente.

Non è concepibile un intervento della terza parte fidata solo al momento della spedizione del messaggio, oppure, come una sorta di "filtro", nel percorso tra spedizione ed arrivo (ad es. ricevendo e ritrasmettendo il messaggio al destinatario, il c.d. *remailer*). In una rete aperta come Internet, i dati trasmessi, tra il punto di partenza ed il punto di arrivo, compiono tortuosi percorsi attraversando molteplici elaboratori di diversa appartenenza, senza alcuna garanzia di effettivo recapito. Pertanto, a tutela del destinatario, è indispensabile che la certificazione della terza parte fidata riguardi proprio il momento finale della trasmissione, cioè il fatto che il messaggio sia stato effettivamente a lui recapitato.

In concreto, poiché il messaggio si considera trasmesso e pervenuto solo quando è memorizzato in una casella di posta elettronica previamente dichiarata dal destinatario, questa funzione certificativa potrebbe essere svolta solo da soggetti che hanno la gestione ed il controllo del sistema di messaggistica del destinatario medesimo. Poiché non sarebbe concepibile attribuire un tale potere certificativo, con effetti opponibili ai terzi, a tutti gli *Internet provider* che gestiscono oggi le caselle di *email*, ne deriva che la certificazione di avvenuta ricezione potrebbe essere emessa solo in caso di trasmissione verso un sistema di posta elettronica gestito sotto il controllo di terze parti fidate autorizzate ad emettere certificazioni di tale specie.

Né darebbe maggiori garanzie la certificazione della chiave del *server* di posta emessa da parte di un certificatore. Tale certificazione, infatti, sarebbe preventiva e generale, non riferendosi alla trasmissione del singolo messaggio. Tra l'altro, è dubbio che possa essere emesso un certificato a nome di un *server* di posta, dato che dovrebbe essere piuttosto emesso a nome dell'ente gestore.

La certificazione della ricezione includerà anche un profilo di validazione temporale, ma non si esaurisce solo nell'aspetto temporale. La marcatura temporale di per sé, infatti, fornisce

certezza giuridica dell'esistenza del messaggio in un certo momento, ma non dà alcuna garanzia circa la sua ricezione da parte del destinatario.

A ben vedere, la situazione non è, poi, così diversa da quanto accade per la trasmissione di un documento cartaceo, per la cui prova della ricezione occorre l'intervento di una terza parte fidata che ne attesti l'effettiva consegna (ad es. postino o ufficiale giudiziario).

L'art. 14 T.U. prevede un'elezione di domicilio informatico, stabilendo che "il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato".

La nozione di indirizzo elettronico, è fissata quale "identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici" (art. 22 comma 1 lett. h T.U.), come ad es. la casella di posta elettronica (*electronic mailbox*) collegata alla rete Internet.

"La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico [...] sono opponibili ai terzi", se si osservano le disposizioni del T.U. e delle regole tecniche (art. 14 comma 2 T.U.).

Tuttavia, oltre queste generiche enunciazioni, si rinvia come al solito a delle regole tecniche che, però, non sono state ancora emanate, non contenendo il d.p.c.m. 8 febbraio 1999 alcun riferimento alla trasmissione del documento. Questo, nonostante che l'art. 1 del decreto affermi espressamente di stabilire, tra l'altro, anche le regole tecniche sulla trasmissione dei documenti informatici.

Il fatto che un documento informatico si intenda pervenuto all'indirizzo elettronico del destinatario non significa, peraltro, necessariamente che esso ne sia venuto a conoscenza. Applicando analogicamente l'art. 1335 c.c. (insieme al collegato art. 1334 c.c.) anche al caso della trasmissione telematica, ne deriva che il destinatario incolpevole può provare di essere stato nell'impossibilità di avere notizia di un documento informatico pervenuto al suo indirizzo elettronico (ad es. per un guasto della rete di collegamento tra *client* e *server* di posta). Il *principio della spedizione* (efficacia della volontà non appena trasmessa all'altra parte), si contrappone al *principio della cognizione* (efficacia della volontà nel momento in cui sia conosciuta dall'altra parte) codificato nell'art. 1326 c.c., con il temperamento della presunzione di cui all'art. 1335 c.c. (*principio della ricezione*).

L'indirizzo elettronico previsto dall'art. 22 comma 1 lett. h T.U. individua uno spazio immateriale; per radicare l'applicazione delle norme che invece presuppongono un riferimento spaziale reale (ad es. norme di diritto internazionale privato, foro competente, ecc.), si potrebbe intendere il riferimento all'indirizzo elettronico come il luogo dove è situata la sede dell'impresa o dell'attività professionale, oppure il luogo dove il titolare dell'indirizzo (se non imprenditore o professionista) ha la sua residenza (argomentando dagli art. 18 e 139 c.p.c. che prevedono come primo criterio la residenza); e questo anche se il luogo dove il messaggio si considera ricevuto è diverso dal luogo dove fisicamente si trova il sistema informatico (*server* o *client* di posta) che ha ricevuto il messaggio.

È stabilito, poi, che "la trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge" (art. 14 comma 3 T.U.). Si fa qui implicito riferimento, oltre che alle norme del codice di procedura civile (art. 149 c.p.c.), anche alla l. 20 novembre 1982 n. 890 ed alla l. 21 gennaio 1994 n. 53, che consentono la notificazione a mezzo del servizio postale.

L'ipotesi normale della notifica telematica comporta un'accettazione del destinatario che sottoscrive una ricevuta con la propria firma digitale. Nel caso in cui il destinatario non intenda firmare una ricevuta e rifiuti il documento o sia irreperibile, l'effetto della notifica, dovrà anche in tali ipotesi basarsi sulla certificazione della terza parte fidata. Una volta che il procedimento di notifica è rispettato, si realizza una conoscenza legale, una sorta di

presunzione assoluta di conoscenza, indipendentemente dalla conoscenza effettiva (a differenza dell'art. 1335 c.c.).

L'art. 14 T.U., per la sua formulazione generale, è da ritenere che ricomprenda anche l'ipotesi della trasmissione di atti giudiziari tra avvocati, consentita dalla legge 7 giugno 1993 n. 183, nonché la notificazione nel processo penale (art. 150 c.p.p.) ed in quello civile (art. 151 c.p.c.), in quanto mezzo idoneo al raggiungimento dello scopo della conoscenza.

3.3 I contratti stipulati con strumenti informatici o per via telematica

In tema di elaboratore e conclusione del contratto, la dottrina distingue:

a) contratti conclusi per mezzo dell'elaboratore, in cui la forma informatica è solo mezzo di esternazione, oppure veicolo di trasmissione, delle dichiarazioni contrattuali già formate e direttamente riconducibili ad una volontà umana;

b) contratti conclusi in automatico dall'elaboratore, in cui la dichiarazione contrattuale è riconducibile ad un elaboratore che la formula in automatico.

L'art. 11 del T.U. stabilisce che "I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge".

La validità dei contratti stipulati in forma informatica (ipotesi *sub a*) con firma digitale, a rigore si desumerebbe già dalle altre norme del T.U. sopra esaminate (in particolare artt. 10, 23 e 24), senza la stretta necessità di una ulteriore norma per stabilirlo. Tra l'altro, la disposizione ricalca, con riguardo ai contratti, l'art. 15 comma 2 della legge n. 59/1997, con l'aggiunta dell'inciso "mediante l'uso della firma digitale".

In base al principio della libertà della forma, la validità dei contratti stipulati in forma informatica *senza firma digitale* (o con firma elettronica semplice) non dovrebbe nemmeno essere messa in dubbio, quando la forma scritta non è richiesta *ad substantiam*. Infatti, il documento informatico esiste ed è tale, anche se senza firma digitale (art. 1 comma 1 lett. b, art. 23 comma 1 T.U.).

Non accettabile è, poi, l'interpretazione che potrebbe scaturire da una rigida lettura dell'art. 11, per cui l'apposizione di una firma digitale sarebbe obbligatoria per la stipula di un contratto con mezzi informatici o telematici, tanto che i contratti che non sono stipulati "mediante l'uso della firma digitale secondo le disposizioni del presente regolamento" sarebbero non validi. In tal caso, significherebbe che per la validità di un contratto per il quale non è richiesta una forma particolare, se è utilizzato lo strumento informatico diventa necessario rispettare le disposizioni sulla firma digitale.

Pertanto, così ragionando la disposizione dell'art. 11 T.U. sembra, piuttosto, una dichiarazione di principio, senza una effettiva portata giuridica. Volendo dare un significato utile, si potrebbe forse pensare che il senso della norma è quello di affermare la rilevanza e validità dei contratti conclusi dall'elaboratore in modo automatico (ipotesi *sub b*), superando così i dubbi espressi dalla dottrina in relazione alla loro ammissibilità per la difficoltà di individuare una volontà negoziale. L'apposizione di una firma digitale per mezzo di una procedura automatica è, peraltro, espressamente prevista dalle regole tecniche, come si è sopra esaminato (art. 1 lett. a, art. 10 comma 2, art. 4 commi 2-3). La dichiarazione contrattuale andrebbe, comunque, imputata, secondo le regole generali, al titolare del relativo certificato.

Il D.P.R. n. 513/1997 stabiliva, con una disposizione che sembrava ugualmente superflua, che "Ai contratti indicati al comma 1 si applicano le disposizioni previste dal decreto legislativo 15 gennaio 1992, n. 50", in materia di contratti negoziati fuori dai locali commerciali (art. 11 comma 2). Infatti, l'art. 9 dello stesso D.LGS. ne stabilisce espressamente l'applicabilità anche "ai contratti conclusi mediante l'uso di strumenti informatici e telematici". La norma, pertanto, in via di interpretazione sistematica, non può

che limitarsi a confermare l'applicabilità del D.LGS. n. 50/1992, mantenendone tutti i presupposti (natura del contratto e dei soggetti). Il D.LGS. n. 50/1992 è, in parte, superato dal D.LGS. 22 maggio 1999 n. 185 di attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza. La tutela si applica ai "contratti a distanza" (art. 2), la cui nozione include i contratti stipulati mediante qualunque idonea tecnica di comunicazione a distanza (nell'elenco esemplificativo dell'allegato I è riportata, tra gli altri mezzi, la posta elettronica). La direttiva n. 97/7/CE non stabilisce particolari modalità per la forma e la comunicazione del diritto di recesso (l'art. 6 disciplina l'ambito, i termini e gli effetti del recesso), affermando che "spetta agli Stati membri determinare le altre condizioni e modalità relative all'esercizio del diritto di recesso" (considerando n. 14). In sede di applicazione non è stata prevista la possibilità di dichiarare il recesso per mezzo di trasmissione telematica di un documento informatico con firma digitale, ritenendo ammissibile solo la comunicazione scritta per mezzo di lettera raccomandata con avviso di ricevimento. (art. 5 comma 4 D.LGS. 185/99). Tale limitazione sembra potersi superare in virtù del vasto ambito applicativo dell'art. 14 T.U.

Il T.U. stabilisce più in generale che "Ai contratti indicati al comma 1 si applicano le vigenti disposizioni in materia di contratti negoziati al di fuori dei locali commerciali" (art. 11 comma 2).

Altre norme specifiche sulla conclusione del contratto con strumenti informatici non sono presenti nel regolamento (ad es. vizi della volontà, tempo e luogo di conclusione, legge applicabile, ecc.), trattandosi di problemi che trovano una migliore collocazione sistematica in un distinto provvedimento normativo. La tendenza a non creare commistioni fra le due discipline (autenticazione dei documenti e conclusione del contratto) è rilevabile anche nei testi normativi stranieri e sovranazionali, in cui manca solitamente qualunque norma relativa ai profili contrattuali. In particolare, la direttiva CE "non disciplina aspetti relativi alla conclusione e alla validità dei contratti" (art. 1), e "non è diretta ad armonizzare le normative nazionali sui contratti, in particolare in materia di conclusione ed esecuzione dei contratti, od altre formalità di natura extracontrattuale concernenti l'apposizione di firme; per tale motivo, le disposizioni sugli effetti giuridici delle firme elettroniche non dovrebbero pregiudicare i requisiti formali previsti dal diritto nazionale sulla conclusione dei contratti o le regole di determinazione del luogo della conclusione del contratto" (considerando n. 17). Questi altri aspetti sono in parte disciplinati dalla direttiva sul commercio elettronico (direttiva n. 2000/31/CE).

I tradizionali problemi del tempo e luogo di conclusione del contratto, della legge applicabile, dell'imputabilità della volontà contrattuale, della forma e dell'errore ostativo nella trasmissione telematiche sono risolvibili con soluzioni che derivano dall'intero impianto del T.U. ed, in ultima analisi, dal fondamentale principio di equivalenza della firma digitale con la sottoscrizione tradizionale. Per quanto riguarda la determinazione del luogo e del momento di conclusione del contratto nelle reti telematiche, si applicheranno, le norme ordinarie in tema di conclusione del contratto tra assenti (artt. 1326 ss. c.c.), riferendole però ad atti preparatori (proposta ed accettazione) in forma informatica, ed all'indirizzo elettronico di cui agli artt. 22 comma 1 lett. h e 14 T.U. Risulta però normalmente impossibile la revocabilità dell'accettazione spedita per via telematica, poiché la revoca non può arrivare prima dell'accettazione stessa (a meno che non si verificano malfunzionamenti del sistema di trasmissione).

Per quanto riguarda eventuali vizi della volontà saranno ancora una volta applicabili le norme ordinarie (artt. 1427 ss. c.c.), dato che la forma informatica con firma digitale non muta la natura delle dichiarazioni. Maggiori problemi in tema di vizi della volontà sorgono per i contratti conclusi in automatico.

Quando è richiesta la specifica approvazione delle clausole vessatorie (art. 1341 comma 2 c.c.), la firma digitale potrebbe, in aggiunta al calcolo sull'intero documento, essere applicata separatamente anche sulle singole clausole vessatorie, o su una dichiarazione autonoma di specifica approvazione, in modo che in seguito si possa provare l'effettiva osservanza della norma. Le clausole vessatorie potrebbero, entro certi limiti, essere riconosciute in automatico dagli elaboratori stessi, mettendo in allarme i sottoscrittori.

Nella documentazione informatica con firma digitale, l'art. 1342 comma 1 c.c. (clausole aggiunte ai moduli o formulari) non può avere applicazione, perché dopo l'apposizione della firma è tecnicamente impossibile aggiungere qualunque altro elemento al documento, in quanto ciò porterebbe ad una mancata verifica tecnica della firma stessa.

Raimondo Zagami

rzagami@notariato.it