

Gianluigi Ciacci

Il Sistema italiano della Firma Digitale e le sue applicazioni pratiche

SOMMARIO: 1. Introduzione. - 2. La firma digitale dal punto di vista tecnico. - 2.1. Le tecnologie crittografiche esistenti. - 2.1.1. Le tecniche di crittografia simmetrica. - 2.1.2. Le tecniche di crittografia asimmetrica. - 2.1.3. Le tecniche di crittografia asimmetrica e la funzione di hash. - 2.2. La Crittografia e la firma digitale. - 2.2.1. La crittografia asimmetrica come criterio di imputazione dei documenti elettronici. - 2.2.2. Dalla crittografia asimmetrica alla firma digitale. - 2.2.3. La figura del soggetto certificatore. - 2.3. La timbratura temporale - 3. Applicazioni pratiche del sistema di firma digitale. - 3.1. Nell'attività dell'avvocato. - 3.1.1 Il fascicolo elettronico. - 3.1.2 L'autentica. - 3.1.3. La comunicazione tra avvocati e la notificazione degli atti giudiziari. - 3.1.4. Il deposito di atti giudiziari. - 3.1.5 La sperimentazione in atto sulla consultazione automatica dei Ruoli e delle funzioni connesse con la liquidazione e registrazione di atti giudiziari. - 3.2. Nell'attività del notaio. - 3.3. Nell'attività del commercialista.

1. *Introduzione*

Per "firma digitale", particolare applicazione della più generale "firma elettronica" (cioè la firma apposta mediante un sistema informatico), si intende la sottoscrizione predisposta sì mediante un elaboratore elettronico, ma sulla base della crittografia a chiave asimmetrica e di particolari funzioni matematiche, come si spiegherà oltre. Tale sistema, in seguito all'organico e completo intervento del legislatore, attraverso disposizioni di carattere generale che hanno radicalmente innovato il quadro normativo di riferimento (nella specie la disciplina giuridica del documento e del documento informatico), viene oggi a costituire il criterio legale di imputazione del documento redatto mediante il computer. Diventa cioè il sistema mediante il quale l'ordinamento giuridico riesce ad attribuire il valore di piena prova alla documentazione prodotta, gestita e trasmessa attraverso l'uso dell'elaboratore elettronico, prescindendo dalla necessità della sua resa cartacea, della sua stampa.

In particolare, si è giunti a tale risultato attraverso un procedimento complesso, ed ancora in fase di realizzazione, in tre diversi momenti:

– innanzitutto con l'art. 15, comma 2, della legge 15 marzo 1997 n. 59 (la cd legge Bassanini 1), che sancisce il fondamentale principio secondo cui "gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione trasmissione con strumenti informatici e telematici, sono validi e rilevanti ad ogni effetto di legge", e precisa che uno specifico Regolamento deve stabilirne "i criteri e le modalità di applicazione";

– successivamente con il D. P. R. 10 novembre 1997 n. 513, appunto il Regolamento richiamato, che introduce quindi una complessa disciplina in 22 articoli, sottoposta a numerose critiche e ad emanazione travagliata, e che procede (artt. 3 e 17 del D. P. R.) ad un ulteriore rinvio per la fissazione delle regole tecniche idonee a renderne effettiva l'applicazione¹;

– infine con il D.P.C.M. 8 febbraio 1999, pubblicato in G. U. 15 aprile 1999, che stabilisce proprio le specifiche tecniche, le regole pratiche del D. P. R. 513/1997, e con il D. P. C. M. che disciplina la figura del certificatore, soggetto fondamentale per la riuscita dell'intero sistema.

Realizzato tale processo, l'Italia diventerà uno dei primi Paesi al mondo ad aver accolto in maniera così integrale l'innovazione tecnologica nel proprio sistema economico-giuridico: e questo proprio attraverso il recepimento della tecnologia della firma digitale per conferire validità giuridica al documento elettronico.

In tal senso è chiarissimo il disposto dell'art. 10 del regolamento citato, norma che, dopo aver previsto al comma 1 la possibilità di apporre o associare ad ogni documento informatico una firma digitale, al comma 2 testualmente prevede: "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". E il documento così redatto assume (art. 5 del D. P. R. 513) il valore di scrittura privata, ai sensi dell'art. 2702 cod. civ., o delle riproduzioni meccaniche, disciplinate nell'art. 2712 del codice civile.

Altra rilevante novità consiste, questa volta per la pubblica amministrazione, nella definizione degli atti e dei documenti informatici delle P.

¹ Un altro rinvio è presente anche nell'art. 4 del D. P. R. ad un decreto del Ministero delle Finanze al fine di disciplinare gli aspetti fiscali dei documenti informatici.

A. come "informazione primaria ed originale, da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni o copie per gli usi consentiti dalla legge" (art. 18, comma I, del D. P. R. 513).

La "rivoluzione", e in particolare la "rivoluzione digitale" (di cui si può in questo caso a ragione parlare, dal punto di vista culturale oltre che giuridico), risiede poi anche nel nuovo concetto di "documento", che prescinde dalla natura, anzi, dall'esistenza stessa del supporto. A ben guardare, infatti, nel documento tradizionale ciò che viene certificato non è l'informazione, ma il supporto che la contiene. Firme, timbri, filigrane, sigilli, persino le barrette metalliche inserite nelle banconote non autenticano l'informazione, ma il supporto. L'autenticità del contenuto è poi data dalla sua inscindibilità dal contenitore.

Ora invece, nel documento informatico, il contenuto digitale è perfettamente separabile dal contenitore e l'autenticazione riguarda proprio lo stesso contenuto.

Ma, in questo come in altri casi in materia di informatica giuridica, non si può prescindere dal dato tecnico, ed occorre quindi esaminare come è stato costruito il sistema della firma digitale a livello informatico.

2. La firma digitale dal punto di vista tecnico

Per ottenere il risultato di assicurare la genuinità dei documenti prodotti attraverso l'uso dell'elaboratore elettronico², genuinità minacciata da diversi fattori, umani o tecnici, sia nel momento della loro conservazione, che in quello della loro trasmissione, sono state adottate soluzioni basate sulla crittografia.

La crittografia è la tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti in una forma illeggibile per quegli utenti che non possiedono una chiave segreta di decifrazione. La funzione è reversibile, per cui l'applicazione dello stesso algoritmo e della chiave segreta al testo cifrato restituisce il testo originale.

Di per sé la crittografia non è una novità. I procedimenti di cifratura

² Infatti anche nel caso del documento informatico, per poter attribuire ad esso efficacia giuridica, si deve preventivamente accertare la sua genuinità e sicurezza: un documento è genuino quando non ha subito alterazioni, mentre è sicuro quando è allo stesso tempo difficile da alterare e, nel caso venga alterato, facile da accertare e da ricostruire.

esistono fin dall'antichità e, come l'etimologia del termine dimostra ("crittografia", dal greco κρυπτος che significa nascosto, celato), fin da allora venivano utilizzati per proteggere i documenti che maggiormente dovevano essere mantenuti segreti. Gli esempi storici sono numerosi, dall'epoca antica ai giorni nostri: dalla "scitala" inviata dai magistrati di Sparta a Lisandro con l'ordine di tornare in patria, descritta da Plutarco nella sua opera "Vite parallele"³; alla manipolazione del testo dei messaggi mandati da Giulio Cesare durante le battaglie in Gallia, usando come tecnica la sostituzione di ogni lettera costituente la parola con altra lettera posticipata nel suo ordine alfabetico⁴; dai banchieri fiorentini del Medioevo, che usavano tecniche crittografiche per proteggere le proprie lettere di credito inviate alle varie filiali; alle macchine "Enigma" utilizzate dai tedeschi durante la seconda guerra mondiale, fondate sull'uso congiunto di una chiave di codifica e di un apposito macchinario a tre (esercito ed aviazione) o a quattro (U-Boot ed unità speciali della Marina) cilindri sequenziali rotanti.

Gli esempi indicati, ed in particolare l'ultimo, mostrano come le tecniche di crittografia siano state applicate soprattutto nell'ambito delle esigenze di segretezza delle informazioni dell'esercito e di quelle diplomatiche: al punto che sono in genere assimilate, per le loro caratteristiche e per l'uso che ne viene fatto, al materiale militare.

È poi l'avvento e lo sviluppo di Internet⁵ quale nuovo *media* di infor-

³ La *scitala* è uno dei pezzi di legno costituenti una coppia di dimensioni uguali, di cui si dotavano due soggetti che volevano scambiarsi messaggi riservati (in questo caso gli efori e Lisandro): il testo del messaggio veniva scritto su un rotolo di papiro (chiamato nello stesso modo del pezzo di legno) avvolto perfettamente intorno alla *scitala*, e che quindi necessitava dell'altra *scitala*, intorno alla quale riavvolgere il papiro come durante la scrittura, per poterlo leggere (così RIDOLFI P., *Dalla "scitala" di Plutarco alla firma digitale*, in *Media duemila*, ottobre 1998, p. 9; dello stesso autore vedi anche *Firma digitale e sicurezza informatica*, Franco Angeli, 1998).

⁴ Usando una posticipazione a base tre, alla lettera A veniva sostituita la D, alla lettera M la P, e così via (questa volta la testimonianza è di Svetonio, nella *Vita dei Cesari*).

⁵ Che comunque ricordiamo nasce per scopi militari (quelli di rendere il sistema di comunicazione tra le varie basi dell'esercito statunitense efficiente e sicuro, non solo in caso di attacco nucleare, ma anche nell'eventualità di un'invasione via terra allo scopo di rendere inservibili o di appropriarsi dei centri di informazione, quali giornali, radio o televisioni; efficienza e sicurezza che si raggiunsero applicando le tecniche della commutazione di pacchetto e del *routing dinamico* alle reti di telecomunicazione) con il nome Arpanet.

mazione e comunicazione, a portare la crittografia ad uscire definitivamente dall'oscurità per essere messa a disposizione di un pubblico sempre più vasto: quello dei milioni di utenti della Rete delle reti, appartenenti a circa 170 Paesi diversi del mondo. Infatti, in questa nuova dimensione rivoluzionaria delle interrelazioni tra individui, un particolare problema consiste nella sicurezza e nella riservatezza dei vari servizi offerti ed utilizzati, uno dei corollari della struttura "aperta" della rete Internet⁶. Tenuto conto del numero sempre maggiore di operazioni commerciali e di trasmissioni di informazioni delicate, quali le informazioni finanziarie o quelle sottoposte al segreto professionale, gli utenti, gli autori e le imprese desiderano garantire, e vedere garantite, proprio tale sicurezza e riservatezza delle informazioni nell'ambito della loro attività svolta su Internet.

Queste nuove esigenze, sicuramente diverse rispetto a quelle dei militari tesi a proteggere le comunicazioni tra gli eserciti, o degli operatori commerciali nell'ambito della propria struttura economica per evitare di rimanere esposti ad attacchi di spionaggio industriale, per essere soddisfatte necessitano di tecniche di crittografia diverse e più evolute: nella specie, tecniche a doppia chiave asimmetrica rispetto a quelle a chiave singola simmetrica.

2.1. Le tecnologie crittografiche esistenti

Volendo operare una distinzione tra le varie tecniche di crittografia esistenti, ci si può basare sul tipo di chiave utilizzato. Così, è possibile individuare due categorie di sistemi crittografici⁷: quelli a repertorio, che sostituiscono a ciascuna parola una determinata serie di lettere e numeri; quelli a cifratura letterale, che provvedono alla sostituzione di lettere (sistemi a sostituzione monoalfabetica), di gruppi di lettere (sistemi a sostituzione poligrammica), o di frazioni di lettere (sistemi tomogrammi)⁸.

⁶ Cioè della sua caratteristica di essere un *media* accessibile a chiunque sia dotato di un computer, di un abbonamento telefonico e di un accesso alla Rete, senza limitazioni, e tendenzialmente senza regole, sia per chi offre servizi ed informazioni, sia per chi ne usufruisce.

⁷ Così GIANNANTONIO E., *Manuale di diritto dell'informatica*, CEDAM, Padova, 1997, p. 377.

⁸ Altri sistemi a cifratura letterale sono quelli a trasposizione letterale e quelli a sostituzione polialfabetica: i primi consistono in una semplice alterazione dell'ordine naturale delle lettere del testo; i secondi, invece, sono caratterizzate da una pluralità di chiavi crittografiche distinte da una lettera, o da una serie di lettere, detta "verme".

Ancora, sempre sulla base del tipo di chiave utilizzato, questa volta con diretta influenza sulla modalità stessa di funzionamento del sistema di crittografia, è possibile distinguere due diversi tipi di tecniche crittografiche: quelle che richiedono l'uso di una sola chiave segreta, la stessa per criptare e decriptare il testo, e perciò dette "simmetriche", e quelle che utilizzano una coppia di chiavi, diverse per "chiudere" ed "aprire" il documento (utilizzate insieme per diverse finalità, come si vedrà oltre), di cui una viene resa pubblica, e dette "asimmetriche".

2.1.1. Le tecniche di crittografia simmetrica

I sistemi di *crittografia simmetrica* funzionano partendo da una medesima chiave, detta "segreta" (perché per la riuscita del sistema tale chiave deve essere conosciuta solo dai suoi utilizzatori), posseduta dall'emittente e dal destinatario di un messaggio, e che serve allo stesso tempo per la cifratura e la decifrazione di un messaggio elettronico⁹. Tale metodo, adatto soprattutto per soddisfare l'esigenza di genuinità del documento nel momento della sua conservazione nelle memorie del computer, e quindi in un momento che si può definire "statico", implica una serie di conseguenze negative che giungono a comprometterne l'efficienza. Il problema di fondo che sorge con la sua utilizzazione è rappresentato, infatti, dalla gestione delle chiavi quando si rende necessario trasmettere il documento a distanza (e quindi nel momento in cui la gestione del documento informatico passa ad essere "dinamica"), dovendo le parti (che si trovano in luoghi diversi) concordare (e scambiarsi) la chiave di criptazione, la cui trasmissione implica ancora un problema di sicurezza: questa infatti potrebbe perdersi, o essere intercettata da un terzo. Inoltre, nel caso di comunicazione con diversi soggetti, si ha la necessità di adottare chiavi diverse per ognuno di essi. Infine, altro aspetto negativo rispetto allo scopo di assicurare l'integrità del documento, è che tale fine si otterrebbe nei confronti di terzi, ma non tra le parti che, essendo dotate della stessa chiave di crittazione, possono entrambe modificare o alterare il documento originario: questo a scapito delle esigenze e delle garanzie di genuinità e sicurezza dell'attività di documentazione¹⁰.

⁹ Il sistema si dice "simmetrico" perché, noti il procedimento e la chiave di codifica, per simmetria si ricavano quelli di decodifica (così RIDOLFI P., *op. cit.*, p. 10).

¹⁰ Necessarie, come si è detto, per attribuire un valore giuridico al documento elettronico.

Esempi di questo tipo di crittografia sono in genere quelli storici già indicati, come quello adottato dalle macchine Enigma durante la seconda guerra mondiale, mentre più di recente si deve segnalare il *Data Encryption Standard (D. E. S.)*, creato dal Governo americano sulla base di una procedura realizzata dall'IBM, riconosciuto come standard internazionale dal *National Bureau of Standards* il 15 luglio 1975¹¹.

Altro importante esempio di crittografia simmetrica è rappresentato¹² dal progetto chiamato "*Escrowed-Encryption Standard (E. E. S.)*", altrimenti conosciuto sotto il nome di "*Clipper*" o di "*Clipper Chip*", sviluppato nell'aprile 1993 dall'Amministrazione presidenziale americana, parzialmente in risposta alla rilevante diffusione del *software* di crittografia asimmetrica P. G. P. (*Pretty Good Privacy*): questo sistema, che potrebbe essere definito di "crittografia fiduciaria", utilizza un algoritmo simmetrico classificato come segreto, messo a punto dalla *National Security Agency (NSA)*, ed è unicamente disponibile su *hardware*. Il termine *escrowed encryption* (o, come si è detto, crittografia fiduciaria) trae la sua origine dal fatto che in tale sistema due agenzie governative, il *National Institute of Standards and Technology (N. I. S. T.)* e il *Department of Treasury*, sono entrambe depositarie di copia di tutte le chiavi installate su *hardware*. In caso di necessità, e a condizione di essere debitamente autorizzato da un mandato di un giudice, un funzionario di pubblica sicurezza potrebbe ottenere una delle chiavi depositate presso tali enti, e procedere quindi alla decifrazione di tutti i messaggi cifrati con l'aiuto di *Clipper*. Nel febbraio 1994, il *Department of Commerce* ha dichiarato che l'*EES* costituiva uno standard federale di crittografia per l'informazione che non è classificata come segreta. L'entità degli ordini fatti dal Governo americano, e l'installazione negli apparecchi di comunicazione quali il fax, il telefono e il modem hanno contribuito a diffonderla su largo raggio e ad elevarla a rango di standard nazionale. Il *Clipper Chip* è stato tuttavia fortemente osteggiato¹³, ed oggi sempre più si tende ad adottare sistemi asimmetrici e ad utilizzare *software* che non

¹¹ Dopo più di venti anni il D. E. S. sembra destinato ad essere sostituito da sistemi più recenti: infatti il NIST ha avviato una selezione del metodo più affidabile fra quindici algoritmi crittografici, che diventerà il nuovo AES (*Advanced Encryption Standard*)

¹² Esempio riportato da HANCE O., *Internet e la legge*, MacGraw Hill, 1997, p. 150.

¹³ Oltre ai già indicati problemi tipici dei sistemi di crittografia simmetrica, il *Clipper Chip* solleva peculiari difficoltà che lo hanno fatto fortemente criticare dagli utenti. Infatti, il ruolo giocato dal NSA, il fatto che depositarie della chiave sono delle agenzie governative, la sua installazione su apparecchi di telecomunicazione e soprattutto la pos-

implichino alcun accesso esterno di autorità governative che possono minare la riservatezza del sistema, rendendolo di fatto inutile, quali ad esempio il P. G. P. .

2.1.2. Le tecniche di crittografia asimmetrica

Come si è detto, la crittografia a chiave segreta, appena esaminata, presentava diversi problemi di gestione e di efficienza. Per questo motivo, e proprio al fine di risolvere gli indicati problemi, nel 1977 vennero inventati i sistemi asimmetrici di criptazione¹⁴, detti anche sistemi a chiave pubblica, resi operativi sotto il nome di RSA (acronimo delle iniziali dei suoi inventori, Rivest, Shamir e Adleman, tre scienziati del *Massachusetts Institute of Technology* di Boston).

In tale ipotesi ciascuna persona risulta in possesso di due chiavi, una pubblica ed una privata: l'algoritmo matematico necessario per la cifratura del documento richiede in questo caso l'applicazione di entrambe le chiavi, comunque con finalità diverse, ora per la criptazione, ora per la decrittazione. Ogni utente che desideri "proteggere" un messaggio ha quindi a disposizione una coppia di chiavi imprescindibilmente connesse¹⁵:

sibilità che esso divenga la sola tecnologia crittografica lecita, fanno temere che il governo federale statunitense acquisisca abusivamente il controllo della trasmissione delle informazioni (così HANCE O., *op. cit.*, p. 151). Nei sistemi a crittografia asimmetrica si pone un problema simile quando viene prevista l'instaurazione di una rete di "terzi fiduciari" (*Trusted Third Parties*). Questi "terzi fiduciari" sarebbero depositari delle chiavi segrete degli utenti di programmi di cifratura e potrebbero trasmettere, previa autorizzazione di un giudice, le chiavi di cifratura alle autorità di polizia al fine di permettere loro di decodificare le comunicazioni intercettate e presumibilmente criminali: costruzione che anche in questo caso, mal si concilierebbe con l'essenza stessa dei sistemi di crittografia.

¹⁴ Asimmetrici perché la chiave di codifica e quella di decodifica sono completamente diverse (e quindi non simmetriche) e non ricavabili le une dalle altre (così RIDOLFI P., *op. cit.*, p. 12).

¹⁵ L'una senza l'altra è inutile. La coppia di chiavi risulta a disposizione dell'utente in seguito alla loro "generazione", attività resa possibile da uno specifico *software* impiegato a tale scopo. Nel programma di crittografia asimmetrica più diffuso al mondo, il *Pretty Good Privacy* (comunemente chiamato P. G. P., è un software di crittografia che utilizza RSA, creato nel 1991 da Phil Zimmermann e distribuito su Internet gratuitamente, ad esempio all'indirizzo web <http://www.alcei.it/pgpalcei.html> consultato il 4 gennaio 1999), si attiva una specifica funzione e si digita una frase casuale a scelta dell'utente, di lunghezza variabile (anche se la sicurezza delle chiavi è direttamente proporzionale ad essa: più è lunga, più le chiavi sono sicure, come lo stesso programma, nelle

una chiave segreta, che custodisce e che gli permette di procedere nella cifratura seguendo dei criteri esclusivi (ciò che consente pertanto di identificare questa persona), e una chiave pubblica, che egli distribuisce a tutti coloro ai quali desidera comunicare i suoi messaggi cifrati¹⁶. La necessità per le parti di scambiarsi informazioni riservate relative al metodo di protezione del documento (e quindi la chiave simmetrica necessaria all'operazione) è eliminata in radice: nella specie, infatti, la chiave privata è destinata a rimanere segreta ed è utilizzabile dal solo legittimo titolare; l'altra chiave deve invece essere resa pubblica con i più diversi mezzi (ad esempio mediante l'inserimento in archivi consultabili anche *on-line*), associandola al nome di un titolare (associazione che sarà garantita da un apposito soggetto, il c. d. *certificatore*).

La crittografia asimmetrica è suscettibile di due distinte utilizzazioni, potendo essere impiegata a fini di segretezza ovvero a scopo di autenticazione¹⁷.

a) crittografia asimmetrica a fini di segretezza

Nella prima ipotesi i messaggi confidenziali potranno essere trasmessi superando i problemi di gestione della chiave, propri dei sistemi simmetrici. Ad esempio A, intendendo inviare un messaggio riservato a B (e quindi un documento che vuole sia letto dal solo B), in primo luogo si procura la chiave pubblica dello stesso B, e quindi cripta il messaggio utilizzando tale chiave; invia poi il messaggio criptato (come tale non comprensibile da alcuno) a B che, ricevuto il messaggio, applica la sua chiave privata (di cui ha esclusiva gestione) per decriptarlo e quindi leggerlo. In sintesi, il mittente cripta il messaggio con la chiave pubblica del

versioni più recenti, simpaticamente avverte): frase che va poi a costituire la password da digitare per "aprire" i messaggi crittografati in base a tale sistema. Il sistema di firma digitale approvato in Italia è invece differente: infatti, secondo il Regolamento tecnico contenuto nel DPCM 8 febbraio 1999, emanato in esecuzione dell'art. 3 del DPR 513/1997, sarà il c. d. "dispositivo di firma" lo strumento attraverso il quale si genereranno le copie di chiavi (così gli artt. 5 e 6 del Regolamento, su cui vedi CIACCI G., *La firma digitale*, Sole 24 Ore Ed., Milano, 1999, pp. 81 e ss.).

¹⁶ Come si vedrà oltre, attraverso l'uso della chiave pubblica di un utente i terzi possono poi anche cifrare un messaggio che quell'utente sarà poi il solo a poter decifrare, ottenendo così la massima riservatezza nell'invio dello stesso.

¹⁷ Per autenticazione si intende un processo in forza del quale il destinatario di un messaggio digitale ha la certezza dell'identità del mittente e/o dell'integrità e non ripudiabilità del messaggio stesso.

destinatario, mentre quest'ultimo, e solo quest'ultimo, decripta il messaggio impiegando la (propria) chiave privata.

b) crittografia asimmetrica a fini di autenticazione

Nella seconda ipotesi, si realizza un risultato particolarmente significativo, consentendo tale sistema l'accertamento della imputabilità, e cioè dell'identità del mittente, e della integrità del messaggio trasmesso, e quindi della sua non ripudiabilità¹⁸: requisito essenziale ai fini della rimozione di uno dei maggiori ostacoli all'effettiva diffusione del commercio elettronico.

Rispetto all'ipotesi che precede, l'impiego delle chiavi (privata e pubblica) risulta invertito, in quanto il mittente cripta il messaggio con la propria chiave privata, mentre il destinatario decripta il messaggio con la chiave pubblica del mittente. Ad esempio A, avendo l'intenzione di inviare a B un messaggio (senza necessità di soddisfare requisiti di segretezza, ma volendolo rendere non modificabile ed assumendosene la paternità), "firma" il messaggio stesso, e cioè applica la propria chiave privata al suo testo e lo spedisce¹⁹; B, ricevuto il messaggio, applica al testo crittato la chiave pubblica di A (prelevata ad esempio, se non già in sua dotazione, da un archivio di chiavi pubbliche) riuscendo quindi a leggerlo. Poiché il messaggio che B decripta applicando la chiave pubblica di A può essere stato criptato solo impiegando la corrispondente chiave privata (la quale si presume sia di esclusiva conoscenza e disponibilità dello stesso A), B avrà la certezza che il messaggio proviene da A e che non ha subito alterazioni dovute ad errori di trasmissione, oppure ad interventi umani; mentre A non può efficacemente sostenere di non avere inviato il messaggio, in genere o con quel determinato testo.

c) crittografia asimmetrica a fini di autenticazione e di segretezza

Si potrebbe poi avere interesse ad applicare entrambe le modalità di

¹⁸ Per il fatto stesso che il messaggio risulta intellegibile dopo aver applicato la chiave pubblica dell'autore, ed è stato quindi spedito effettivamente dal mittente titolare della chiave privata, significa che non è stato alterato (così RIDOLFI P., *op. cit.*, p. 12).

¹⁹ Come si vedrà oltre, avendo presente la funzione essenziale della sottoscrizione (autografa), quella di associare un testo al suo autore, e quindi la sua natura di essere tradizionalmente il criterio di imputazione di un documento, e considerando che l'uso della chiave privata in un sistema di crittografia asimmetrica ottiene lo stesso risultato, anche se forse fuorviante per la comprensione immediata dell'intero sistema, non è completamente errato usare il termine "firma" per indicare tale operazione.

crittografia asimmetrica al documento informatico che si vuole trasmettere, per ottenere la certezza dell'autenticazione e della riservatezza dello stesso: si immagini l'ipotesi di un contratto concluso a distanza tra due soggetti che utilizzano un sistema di posta elettronica²⁰. In questo caso il mittente cripterà il messaggio due volte: prima con la propria chiave privata, per assumerne la paternità; poi con quella pubblica del destinatario, per essere sicuro che solo quest'ultimo, grazie alla sua chiave privata, sarà in grado di leggerlo, ed ottenere quindi la riservatezza dell'avvenuto accordo. Colui che riceve il messaggio "protetto" due volte compierà l'operazione inversa: e quindi applicherà prima la sua chiave privata, otterrà un testo ancora illeggibile, al quale applicherà la chiave pubblica del mittente, riuscendo infine a leggere il testo originario.

Evidenti risultano i vantaggi dei sistemi a chiave pubblica rispetto a quelli simmetrici. In primo luogo, eliminata la necessità di trasmissione della chiave segreta, con i primi si realizza un maggior grado di sicurezza. In secondo luogo, attraverso la chiave privata, i soli sistemi asimmetrici consentono l'accertamento dell'imputabilità e dell'integrità del messaggio trasmesso, e assicurano la funzione del non ripudio, non potendo il mittente negare di avere inviato un messaggio (o un messaggio con un determinato contenuto) ove lo stesso sia stato crittato con la sua chiave privata, azione che si presume sia possibile solo al titolare della stessa. Sulla base di tale presunzione, che per questi sistemi può considerarsi assoluta²¹, l'unico problema di sicurezza che si potrebbe presentare riguarda l'autenticità della chiave pubblica, vale a dire la garanzia che

²⁰ E che hanno l'esigenza di scambiare una corrispondenza (nella specie la proposta negoziale e l'accettazione della stessa, o altre comunicazioni attinenti alla fase di trattativa) riservata, in cui entrambe possano essere sicure della provenienza e non ripudiabilità delle varie dichiarazioni.

²¹ Anzi, *deve* essere ritenuta assoluta, altrimenti non potrebbe funzionare: è l'applicazione di un principio di autoresponsabilità che l'utente si assume nel momento in cui decide di utilizzare il sistema (così come, più o meno consapevolmente, chi guida l'automobile accetta l'applicazione dell'art. 2054 c. c., in materia di circolazione di veicoli "senza guida di rotaie", e si assume i rischi dell'inversione legale dell'onere della prova in caso di incidente), che si esaurisce solo quando lo stesso chieda al soggetto competente la revoca delle certificazioni relative alle chiavi, in caso ne abbia perduto il possesso o siano risultate difettose (così secondo l'art. 8, comma IV, lett. c del DPCM 8 febbraio 1999). Se così non fosse, nessun affidamento si potrebbe fare sul messaggio crittato con la chiave privata del mittente (questo il motivo per cui non è chiara la previsione della possibilità di autenticare il risultato dell'attività di criptazione, stabilita nell'art. 16 del DPR 513/1997). Sul punto si veda CIACCI G., *op. cit.*, pp. 133 e ss. .

la chiave pubblica provenga effettivamente dall'utente, previamente identificato²², e che non sia stata contraffatta. Questo problema è risolto attraverso la creazione di un ente di autenticazione che si renda garante, nei confronti dei terzi, dell'autenticità della chiave pubblica, e cioè della corrispondenza chiave-soggetto titolare, correttamente identificato: ente che assume quindi un'importanza fondamentale in questi sistemi, chiamato "Certificatore" o "Autorità di certificazione", e di cui si parlerà oltre.

2.1.3. Le tecniche di crittografia asimmetrica e la funzione di hash

Segnalati gli aspetti positivi dei sistemi asimmetrici, deve però rilevarsi che la criptazione a chiave simmetrica risulta essere più rapida e veloce, soprattutto nel caso di documenti particolarmente lunghi, che tra l'altro sono anche maggiormente esposti ad una possibile violazione.

Al fine di ovviare a tale inconveniente, nei sistemi a criptazione asimmetrica è stata ideata un'ulteriore metodologia di protezione dei documenti informatici: la chiave privata, infatti, non viene applicata di regola sull'intero messaggio, ma solo su di un estratto di esso, una specie di sintesi che viene automaticamente ricavata dal documento originale applicando una funzione di *hash*²³.

Tale tecnica rende possibile, partendo da un determinato documento di lunghezza variabile, ottenere una sequenza di caratteri alfanumerici a lunghezza prefissata e standard (normalmente a 128 o 160 *bit*), una stringa definita "impronta" (o *hash code*): questo tramite l'applicazione al testo

²² Al quale si presume essa appartenga, essendo la seconda parte della coppia di chiavi.

²³ Nel DPCM 8 febbraio 1999, la funzione di *hash* viene definita come "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" (esempi di algoritmi di generazione dell'impronta, che costituiscono la citata funzione matematica destinata a generarli, sono MD2, MD4, MD5, SHA-1, RIPEMD); mentre per "impronta" si intende "la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di *hash*" (così dall'art. 1 dello Schema di regolamento). Una dottrina considera poi l'*hash* un terzo tipo di funzione di crittografia, oltre a quella simmetrica ed a quella asimmetrica (FAGNANI M., *Firma digitale: soluzioni e strumenti per la realizzazione, problematiche gestionali*, intervento al Convegno *I regolamenti di attuazione in materia di firma elettronica e archiviazione ottica dei documenti*, Roma, 25 e 26 novembre 1998).

del documento di un algoritmo matematico (la c. d. "funzione di *hash*") che, sulla base del numero e del tipo di caratteri, permette di generare tale estratto. È importante sottolineare che l'impronta è unica per ogni documento, e che basta cambiare anche un solo carattere del testo dello stesso (anche solo uno spazio), per avere un'impronta diversa²⁴.

Queste caratteristiche rendono tale modalità fondamentale ai fini dell'apposizione della firma digitale ad un documento, come si vedrà oltre: è infatti la commistione tra una funzione matematica (l'*hash*) e la crittografia asimmetrica a permettere di ottenere un ottimale livello di efficienza, e ad essere utilizzata nei più recenti sistemi di firma digitale. Anzi, nonostante che già i sistemi di crittografia asimmetrica, nella loro funzione di autenticazione, rendano possibile imputare un determinato documento elettronico al soggetto che vi applica la propria chiave privata (che può essere quindi considerato il firmatario di quel documento), solo l'integrazione con i sistemi di *hash* permette di parlare di "firma digitale".

Così, ad esempio, dovendo A trasmettere a B un documento con numerose pagine ed allegati, non applica immediatamente la sua chiave privata, ma prima esegue l'*hash*, ottenendo come risultato un testo di poche righe di per sé incomprensibile, che sarà il solo ad essere criptato: in questo modo firma digitalmente il documento²⁵. Invia quindi il tutto²⁶ a B che, dopo aver prelevato la chiave pubblica di A, la applica alle righe dell'*hash* criptato all'interno del testo ricevuto, e ottiene dunque l'*hash* in chiaro; B prenderà a questo punto il testo originario a cui è allegato l'estratto, ne ricaverà l'impronta in base alla stessa funzione di *hash* (si

²⁴ Ad esempio, un testo che contenesse una frase di questo genere:

"accetto di acquistare 3 libri a 60.000 lire"

genererà un'impronta totalmente diversa da questo altro testo:

"accetto di acquistare 6 libri a 30.000 lire"

nonostante esso contenga lo stesso numero e lo stesso tipo di caratteri.

²⁵ Anche in tal caso, quindi, basta solo modificare un carattere affinché cambi l'impronta, e di conseguenza la firma digitale: nell'indicato sistema non si avrà dunque una sottoscrizione unica per tutti i documenti di un autore (a parte le variazioni calligrafiche), ma tante firme digitali, tutte validi criteri di imputazione, quanti sono i diversi documenti sottoposti a funzione di *hash* e crittografia mediante chiave privata.

²⁶ E cioè il documento originario intero e leggibile con alla fine la stringa dell'*hash* criptata dalla chiave privata di A: in questo caso, vista la similitudine con i metodi tradizionali di sottoscrizione, si è in presenza di un documento informatico con firma digitale, almeno secondo il costrutto introdotto dal legislatore italiano con il DPR 513/1997.

ricorda che le funzioni di *hash* sono di pubblico dominio, ed anzi sono preventivamente scelte dallo stesso legislatore²⁷), e quindi confronterà tale impronta con quella ricavata dal messaggio di A, ottenendo in questo modo, nel caso di una perfetta coincidenza tra le due stringhe, la sicurezza della genuinità e della provenienza del documento elettronico. Se poi tale documento è un contratto, a prescindere dalla sua lunghezza, l'apposizione in calce al testo dello stesso della stringa costituente l'impronta (cioè il risultato della funzione di *hash* sul testo)²⁸, implicherebbe l'accettazione del suo contenuto: in questo caso l'applicazione di funzione di *hash* e di chiave pubblica del mittente risulterebbe necessaria per essere certi della provenienza e non ripudiabilità, oltre della non alterazione del testo, e quindi della validità dello stesso negozio.

Allo schema appena indicato, per l'apposizione e la verifica della firma digitale, si può aggiungere anche l'altra applicazione della crittografia asimmetrica, quella a fini di segretezza. Infatti, se si volesse mantenere anche riservato l'intero documento (cioè il testo originario leggibile integrato con l'impronta criptata attraverso la chiave privata di A per soddisfare le indicate esigenze di autenticità), si potrà a sua volta criptare con la chiave pubblica di B. In questo caso B prima applicherà la propria chiave privata, ottenendo il documento originario (e cioè il testo leggibile e l'impronta criptata); poi applicherà la chiave pubblica di A al solo *hash* criptato, ottenendo l'*hash* in chiaro; applica infine la funzione di *hash* al testo originario leggibile, ottenendo un'impronta; a questo punto confronterà tale impronta con quella risultata dalla decrittazione con la chiave pubblica di A, e se le due impronte coincidono sarà sicuro della genuinità e della autenticità del documento.

Alla luce delle varie applicazioni appena indicate, si può rilevare la

²⁷ Nel DPCM 8 febbraio 1999 le funzioni di *hash* accettate sono, come già indicato, MD2, MD4, MD5, SHA-1, RIPEMD.

²⁸ Magari ripetuta due volte, la seconda per le clausole vessatorie che devono essere specificamente approvate ai sensi dell'art. 1341 c. c. . È chiaro che quest'ultima costruzione che si sta esponendo (ma che poi è probabilmente quella tenuta presente dal legislatore nella realizzazione del sistema di firma digitale previsto dal DPR 513/1997) è ancora troppo legata ad una concezione "testuale" dei documenti informatici (sembra cioè implicare ancora la stampa, o comunque la visualizzazione, degli stessi, dalla quale si riscontra la presenza dell'impronta alla fine del foglio; mentre si dovrebbe considerare il solo *file*, che potrebbe nemmeno essere stampato), ma si ritiene potrà essere comunque un valido strumento per una prima fase di utilizzo del sistema, gettando una specie di ponte tra il "vecchio" e il "nuovo".

mutata funzione della crittografia nell'attuale sistema economico, sempre più proiettato verso la comunicazione e l'informazione automatica, e verso il nuovo mercato del commercio elettronico; nata cioè come strumento per nascondere ciò che è stato scritto, viene applicata per tutt'altri scopi: garantire che quello che è scritto non è stato alterato, per dolo o incidente, e che la firma che appare è autentica²⁹.

2.2. La Crittografia e la firma digitale

La descrizione relativa alle tecniche di cifratura per proteggere i documenti informatici rende possibile rilevare come i moderni sistemi di crittografia asimmetrica, creati al fine di risolvere problemi pratici legati allo svolgimento di diverse attività attraverso le moderne reti telematiche, in particolare attraverso Internet, permettano, a causa della loro stessa struttura, di trovare una soluzione anche ai problemi di natura completamente diversa: nella specie, quelli legati alla validità giuridica dei documenti prodotti e gestiti attraverso l'elaboratore elettronico.

2.2.1. La crittografia asimmetrica come criterio di imputazione dei documenti elettronici

Infatti, se si considera l'importanza data dal nostro ordinamento giuridico alla sottoscrizione quale criterio di imputazione delle dichiarazioni provenienti da un determinato soggetto, ponendola a fondamento del valore probatorio conferito ad alcune specie di documenti (come, ad esempio, la scrittura privata o l'atto pubblico), ed allo stesso tempo si riflette sul fatto che tale importanza deriva dall'efficacia (almeno teorica) della stessa a raggiungere quel fine (l'imputazione), un sistema che ottenesse il medesimo risultato (la certezza della provenienza delle dichiarazioni contenute in un documento) potrebbe acquisire anche la medesima importanza. Sulla base di tale assunto si può allora affermare che, permettendo la tecnica di crittografia asimmetrica di avere la certezza assoluta sull'identità dell'autore di un determinato documento elettronico (e quindi ottenendo lo stesso risultato della sottoscrizione autografa per i documenti tradizionali), di conseguenza anche i documenti prodotti e gestiti mediante elaboratore elettronico, su cui si è applicata la chiave segreta di un soggetto a fini di autenticazione, possono essere considerati equiva-

²⁹ Così RIDOLFI P., *op. cit.*, p. 12.

lenti a (cioè con lo stesso valore giuridico di) quelli cartacei. La crittografia a chiavi asimmetriche costituisce quindi un criterio valido di imputazione dei documenti elettronici; ai quali deve dunque essere riconosciuto lo stesso valore di quelli cartacei tradizionali: documenti scritti, atti pubblici, scritture private o riproduzioni meccaniche "a seconda di come siano rogati"³⁰.

Sulla base di queste conclusioni si è proceduto alla costruzione di strutturati sistemi, riconosciuti anche a livello legislativo³¹, che hanno permesso di fare entrare "a pieno titolo" nell'ordinamento giuridico dei vari Paesi anche le nuove forme di documentazione. Talvolta sulla base semplicemente della tecnica di crittografia asimmetrica descritta, altre volte associando alla stessa anche la modalità connessa all'uso della funzione di *hash*, ipotesi in cui si è parlato di "firma digitale".

2.2.2. Dalla crittografia asimmetrica alla firma digitale

In particolare, si è introdotta una distinzione tra le due possibilità nonostante logicamente, e sulla base della natura stessa dei sistemi impiegati³², in entrambi i casi la funzione di imputazione venga confermata: da una parte, quella rappresentata dalla criptazione mediante il solo uso della propria chiave privata; dall'altra, la previa generazione dell'impronta e quindi, successivamente, la criptazione unicamente di questa con la chiave privata. Secondo i sistemi che adottano questo tipo di distinzione,

³⁰ Così in BORRUSO R., *La tutela del documento e dei dati*, in AA. VV., *Profili penali dell'informatica*, cit., p. 13. È chiaro che per conseguire un risultato così importante non è sufficiente l'interpretazione, seppur apparentemente inconfutabile, della dottrina, ma occorre un riconoscimento legislativo: e la novità risiede proprio in questo, nella nuova consapevolezza acquisita dal legislatore che via via accoglie e disciplina nei vari Paesi le nuove modalità di documentazione.

³¹ Dalle discipline emanate in Utah, Illinois, Florida, Georgia e Washington, attraverso l' "Information and Communication Services Act - Informations und Kommunikationsdienste-Gesetz - IuKDG" tedesco del 1 agosto 1997, fino al nostro D. P. R. 513/1997, ed alle recenti esperienze di Singapore con il *Singapore Electronic Transactions Act* del 29 giugno 1998.

³² In ogni caso la crittografia asimmetrica, ma quando si utilizza la funzione di *hash* è solo l'impronta ad essere sottoposta a cifratura, mentre viene mantenuta (ed anzi in tal senso sembrano strutturati i più recenti sistemi di firma digitale, come quello italiano) la parte "in chiaro", cioè non criptata, del documento originario. A questo proposito valgono i rilievi fatti in precedente nota, circa l'eccessivo legame ai sistemi tradizionali cartacei nella concezione della tecnica.

unicamente nel secondo caso si sarebbe in presenza di una firma digitale.

Come si è detto in precedenza, il Legislatore italiano ha introdotto nel nostro Paese un'articolata³³ disciplina in materia di valore giuridico del documento elettronico, sulla base proprio della firma digitale; anche se poi deve rilevarsi che, almeno con riferimento al solo DPR 513, non si capisce bene quale delle due modalità di crittografia asimmetrica indicate venga effettivamente scelta, e se devono essere considerate alternative o cumulabili: e questo nonostante che un'intera parte del D. P. R. 513 (il capo II), oltre ad alcune specifiche norme, espressamente riportino proprio la dizione "firma digitale". Tale difficoltà di comprensione è frutto della confusione fatta tra l'uso della chiave privata e la sottoscrizione digitale³⁴: confusione che viene poi chiarita dal Regolamento tecnico, emanato ai sensi dell'art. 3 del DPR 513, attraverso l'introduzione della funzione di *hash*.

Vista la complessità dell'argomento, occorre però procedere con ordine, e attraverso l'esame del complesso sistema italiano al fine di comprendere quale metodologia di firma verrà utilizzata per conferire valore giuridico al documento informatico, si chiarirà anche come funziona in pratica la tecnica di sottoscrizione elettronica.

Innanzitutto, si può partire dalla pacifica affermazione circa il recepimento, nel DPR 513/1997 del sistema di criptazione asimmetrica: come si può evincere dalla lettura dell'art. 1 che riporta le definizioni dei termini usati nel Regolamento, dove si parla espressamente di "sistema di chiavi asimmetriche a coppia" (art. 1, lett. *b*, *d*, *e* ed *f* del D. P. R. 513).

³³ Si è indicato, infatti, come ciò sia avvenuto attraverso una specie di "fattispecie a formazione progressiva" rappresentata dall'emanazione successiva dell'art. 15, comma II, della l. 15 marzo 1997 n. 59, in materia (tra l'altro) di riforma della P. A. e di semplificazione amministrativa, del D. P. R. 20 novembre 1997, n. 513 (il "Regolamento contenente i criteri e le 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"), e delle Regole Tecniche in esecuzione dell'art. 3 del DPR 513, in corso di approvazione da parte della Presidenza del Consiglio dei Ministri (deve ricordarsi, a completare questa fattispecie, anche il decreto del Ministero delle Finanze che, secondo l'art. 4 comma II del DPR 513, dovrà disciplinare gli "obblighi fiscali relativi ai documenti informatici").

³⁴ Segnalata anche da Martino che rileva come ciò sia "grave, e contrario agli orientamenti della UE e giuridicamente sbagliato: ed è tanto grave che è una delle ragioni del ritardo nella pubblicazione dopo la firma del decreto" (MARTINO A. -a cura di-, *Nuovo regime giuridico del documento informatico*, Franco Angeli, 1998, p. 24).

Inoltre il Legislatore ha considerato entrambe le utilizzazioni ricordate della crittografia asimmetrica (a fini di segretezza, ovvero a scopo di autenticazione), avendo espressamente prevista la possibilità di utilizzare la chiave privata per apporre la firma digitale ovvero per decifrare il documento già criptato con la corrispondente chiave pubblica da parte di un altro soggetto (art. 1 lett. e del DPR 513), nonché la utilizzabilità della chiave pubblica per verificare la firma digitale ovvero per criptare i documenti da inviare (art. 1 lett. f del DPR 513, chiaramente, in quest'ultimo caso, chiave pubblica di un altro soggetto). Per quanto riguarda poi il problema indicato, in mancanza di alcuna norma che espressamente distingua tra la cifratura mediante l'uso della chiave privata e la sottoscrizione digitale, sembrerebbe accolta la seconda modalità, quella attraverso la funzione di *hash*, sulla base dell'interpretazione degli articoli in cui si usa l'espressione "apposizione" di firma digitale (ad esempio l'art. 6, comma II, o l'art. 10, comma I, in cui viene anche prevista l'ulteriore operazione di *associarla al documento informatico con separata evidenza informatica*, a scapito anche in questo caso della comprensibilità del costruito). Di fatto, sulla base della lettura del solo DPR 513, avendo ben chiara la funzione di imputazione delle dichiarazioni elettroniche delle tecniche di crittografia asimmetrica, non si riusciva bene a comprendere come in pratica si dovesse procedere ad "apporre" una firma digitale³⁵.

Diversa la situazione in seguito all'emanazione l'8 ottobre 1999 con Decreto del Presidente del Consiglio dei Ministri, delle "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513". Infatti, fin dall'art. 1 dell'Allegato

³⁵ Si vedano, ad esempio, l'art. 1, lett. e del DPR 513, che definisce la chiave privata come "l'elemento della coppia di chiavi asimmetriche (...) mediante il quale si appone la firma digitale sul documento informatico"; l'art. 10, comma I, che usa (come si è detto) le espressioni "apposizione" o "associazione con separata evidenza informatica" della firma digitale e, ancora, l'art. 10 comma IV, che dispone che "per la generazione della firma digitale deve adoperarsi una chiave privata". In nessun caso si parla quindi della funzione di *hash*, né direttamente, né attraverso la descrizione delle modalità di funzionamento; anzi, i termini impiegati sembravano indicare che il Legislatore si riferisse solo all'operazione di criptazione mediante l'applicazione della chiave privata del soggetto al documento informatico (unica possibilità di "adoperare" una chiave privata), e "firma digitale" fosse il risultato della stessa.

Tecnico di tale regolamento³⁶, contenente le definizioni usate nel testo, è possibile comprendere il sistema di firma digitale scelto dal Legislatore italiano: quello basato sulla crittografia a chiavi asimmetriche unita alla funzione di *hash*; questo perchè vengono introdotti sia il concetto di "impronta", sia quello di "funzione di hash", e ad essi si aggiungono, per meglio identificare le modalità pratiche di svolgimento dell'attività di sottoscrizione digitale, quello di "dispositivo di firma" e di "evidenza informatica"³⁷. Inoltre sono dettate una serie di disposizioni che avvalorano la conclusione indicata circa il sistema di firma adottato nel nostro Paese: si vedano in particolare l'art. 3, intitolato "algoritmi di *hash*", che specifica dal punto di vista tecnico quale funzione si debba utilizzare per la generazione dell'impronta; l'art. 4, comma IV, lett. a, che, nello specificare le tipologie di chiavi e servizi utilizzate nel sistema costruito dallo stesso Regolamento, parla di "chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti"; l'art. 10, comma III, che in materia di modalità di generazione e verifica delle firme, dispone che "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".

Così, nonostante il testo indicato non si caratterizzi certo per chiarezza, coerenza della costruzione giuridica e completezza, è ora possibile tentare di descrivere come avviene una sottoscrizione digitale.

Innanzitutto il soggetto deve predisporre per l'utilizzo del sistema, e quindi dotarsi di una stazione operativa informatizzata, e munirsi dell'opportuno software per l'attività di firma. Questo, probabilmente fornito dallo stesso ente che successivamente svolgerà la fondamentale funzione di garantire l'associazione chiave-titolare, dovrà permettere la generazione della coppia di chiavi, dovrà contenere la funzione di *hash*, e

³⁶ La forma legislativa impiegata è quella di un decreto della Presidenza del Consiglio dei Ministri, costituito di due articoli, con un "Allegato tecnico" di 63 articoli suddivisi in cinque capi, che contiene il vero e proprio Regolamento (l'espressione usata nell'art. 2 del DPCM è la seguente: "le regole tecniche, di cui all'articolo 1, sono riportate nell'allegato tecnico del presente decreto").

³⁷ Ai sensi dell'indicato articolo, oltre alle definizioni già riportate in precedente nota di "impronta" e di "funzione di hash", per "dispositivo di firma" deve intendersi "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"; mentre "evidenza informatica" deve essere considerata "una sequenza di simboli binari che può essere elaborata da una procedura informatica".

quindi rendere possibile l'apposizione delle firme digitali: probabilmente queste esigenze verranno soddisfatte da un sistema di *smart card*, che maggiormente sembrano incontrare i requisiti richiesti dal Regolamento tecnico quando parla di "dispositivo di firma"³⁸. Una volta creata la coppia di chiavi, l'utente dovrà renderne pubblica una delle due attraverso la procedura di certificazione, per il corretto funzionamento del sistema; tale procedura consiste nella richiesta presentata ad uno dei soggetti che svolgono la funzione di certificatori delle chiavi pubbliche, iscritti nell'elenco tenuto a cura dell'A. I. P. A., di attestare la corrispondenza chiave-titolare, di rilasciare quindi il certificato (che dovrà essere allegato ogni volta in cui il soggetto appone la propria firma digitale), e di pubblicarlo insieme alla chiave pubblica nell'elenco delle chiavi di sua gestione, elenco che sarà posto *on-line* a disposizione di chiunque voglia accertare la provenienza di un determinato documento elettronico cifrato mediante l'utilizzo della chiave privata di uno dei soggetti clienti dello stesso certificatore. Terminata con questa operazione la fase preparatoria dell'uso del sistema di firma digitale, l'utente è pronto a sottoscrivere i propri documenti nell'ambito della sua attività di documentazione, sia essa statica o dinamica.

Così, ipotizzando si decida di inviare una determinata dichiarazione in forma elettronica ad un altro soggetto, volendogli conferire la certezza di contenuto e provenienza, si dovrà, mediante il dispositivo di firma, ricavare l'impronta della stessa, e quindi, sempre mediante lo stesso di-

³⁸ Le *carte intelligenti* o "*smart card*" sono un particolare tipo di carte elettroniche, senza dubbio il più evoluto (al loro interno presentano infatti uno o più microcircuiti che consentono la memorizzazione e l'elaborazione di dati, ed in particolare sono dotate di un chip contenente: un microprocessore, una memoria RAM, una ROM, e di adeguate interfacce per l'alimentazione e il dialogo con altri sistemi), e rappresentano oggi uno dei simboli più interessanti del sempre più diffuso processo di informatizzazione della moderna società. Di difficile e costosa duplicazione, considerate virtualmente inviolabili, sono in grado di memorizzare ed elaborare dati in modo estremamente sicuro; vengono utilizzate sia come contenitori di dati personali (ad esempio i dati sanitari, i libretti universitari, documenti di identità, ecc.), sia in campi quali la monetica (cioè il pagamento elettronico di beni e servizi ed i trasferimenti elettronici di fondi), i controlli di accesso alle banche dati ed a servizi di varia natura, e la protezione del software e dei dati, essendo in grado di svolgere funzioni di identificazione, di autenticazione e di protezione crittografica dei messaggi. L'identificazione del portatore di una "Smart card" può essere eseguita interamente all'interno della carta stessa, grazie ai dati contenuti nell'area di memoria segreta: questo consente di identificare in modo sicuro la validità del codice personale P. I. N. (*Personal Identification Number*), fornito dal portatore della carta.

positivo, applicare la propria chiave privata: ottenendo in questo modo la "generazione" della firma, cioè di quella determinata stringa che sarà il risultato dell'impronta di *hash* crittografata (con aggiunto il certificato), che potrà poi essere apposta in calce al testo oggetto del procedimento, oppure associata a questo. Chi riceverà il messaggio risultato dell'operazione di sottoscrizione elettronica, procederà all'apertura e/o verifica dello stesso, mediante il proprio dispositivo di firma. Tale dispositivo, agendo sul documento criptato, acquisirà dal certificato annesso al documento firmato l'indirizzo del certificatore che lo ha emesso, e quindi, se non si trova già in possesso della chiave pubblica del mittente (o in caso questa risulti troppo datata, o per essere comunque sicuro che non sia stata nel frattempo revocata o sospesa), si collegherà alla risorsa telematica del certificatore (il suo sito *web* su Internet, oppure direttamente al suo elaboratore attraverso una connessione telematica diretta) per prelevare la chiave pubblica e controllare la validità del certificato; a questo punto, applicando la chiave pubblica del mittente, "aprirà" il documento informatico ricevuto, ottenendo quindi l'impronta di *hash*; calcolerà poi dal testo originario a sua volta l'impronta, e dunque confronterà le due versioni: se coincidono sarà allora sicuro della provenienza e della genuinità del messaggio.

È chiaro che quasi sicuramente la complessa procedura indicata verrà resa molto semplice dai software di firma digitale e, come si usa dire, "*friendly*" per gli utenti: anzi molto probabilmente tale requisito, la semplicità d'uso, sarà uno dei punti fondamentali per la riuscita dell'intero progetto³⁹. Così, una volta espletate le formalità iniziali relative alla procedura di certificazione, l'attività del soggetto che firma, come quella del soggetto che vuole leggere un documento "firmato", nel caso il dispositivo di firma sia rappresentato da un software, consisterà essenzialmente nell'attivare qualche funzione del proprio programma di posta elettronica o di video scrittura; nel caso invece si realizzerà un sistema di dispositivi di firma attraverso *smart card*, sia per apporre la propria sottoscrizione digitale, sia per verificare quella dei propri corrispondenti, l'utente inserirà semplicemente la propria carta "intelligente" in un appo-

³⁹ Altro requisito, oltre all'apparente utopica attività di snellimento delle procedure burocratiche della P. A., che si ritiene di rilevante importanza, è quello dell'investimento in cultura delle nuove tecnologie: sarà infatti solo grazie all'acquisizione di una cultura informatica che sarà possibile controllare le rivoluzionarie innovazioni introdotte nella società dall'informatica e dalla telematica.

sito lettore, che lavorerà sempre insieme ai programmi di video scrittura o di gestione della posta per svolgere le indicate operazioni.

A prescindere comunque dalla procedura che sarà in pratica adottata, la descrizione appena fatta permette di rendersi conto della fondamentale rilevanza che assume il soggetto certificatore in un sistema di firma digitale, come quello adottato dal DPR 513.

2.2.3. La figura del soggetto certificatore

Si è già sottolineato che è di basilare importanza, per il funzionamento dei sistemi di crittografia a doppia chiave, che una delle due chiavi venga resa pubblica, insieme all'attestazione della sua complementarità a quella che rimane segreta e del fatto che il suo titolare sia effettivamente la persona che dice di essere: si deve cioè rendere conosciuta dal maggior numero di persone possibili, con la garanzia che sia veramente Tizio il suo titolare, e che effettivamente corrisponda all'altra parte della chiave, quella privata.

Il richiamato problema relativo alla certezza della corrispondenza tra chiave pubblica e soggetto titolare cui essa appartiene viene in genere risolto attraverso la costruzione di specifici sistemi di certificazione (detti P. K. I., cioè *Public Key Infrastructure*), in base ai quali si ottengono le garanzie indicate. Tali sistemi si basano in genere sull'attività di soggetti (le c. d. *trusted third party*, cioè i certificatori o le Autorità di certificazione), pubblici o privati, che svolgono la funzione di identificare il titolare della chiave pubblica, rilasciare un certificato digitale che attesti tale riconoscimento, e in genere metterlo a disposizione dei terzi insieme alla stessa chiave pubblica, attraverso l'inserimento in un elenco consultabile *on-line*. Essi sollevano poi interessanti questioni, sia giuridiche che tecniche, relative al loro funzionamento: così, dal primo punto di vista, devono essere tenuti presenti, ad esempio, i problemi della responsabilità per il realizzarsi di eventuali danni connessi all'uso delle chiavi di crittografia dei propri clienti; dal punto di vista tecnico, invece, si devono prevedere specifiche disposizioni sulla sicurezza di tali sistemi, e scegliere la loro struttura gerarchica. Infatti, relativamente a questo ultimo punto, è possibile distinguere tra due diversi approcci: quello che prevede una struttura gerarchica orizzontale, nel quale l'attestazione della corrispondenza chiave-titolare avviene ad opera degli altri utenti del sistema, senza quindi uno specifico soggetto a cui tutti si riferiscono⁴⁰; e

⁴⁰ È questo il sistema del più diffuso programma di crittografia asimmetrica, il P. G.

quelli a struttura verticale, in cui esiste un soggetto certificatore che accerta l'indicata corrispondenza e pubblica certificati e chiavi, a sua volta facente capo ad un'autorità centrale, che certifica le sue chiavi e quelle degli altri soggetti che svolgono la medesima funzione. È questa la struttura recepita nei sistemi di firma digitale più recenti, riconosciuti in genere dal Legislatore.

Per quanto riguarda il nostro Paese, come si è detto il D. P. R. 513/1997 ha espressamente legato il riconoscimento della piena validità e rilevanza del documento informatico alla necessaria adozione di un sistema di crittografia a chiavi asimmetriche con chiave pubblica certificata, attraverso una procedura gestita e garantita da apposite Autorità⁴¹. Queste possono essere soggetti pubblici e privati, che offrano opportune garanzie di "stabilità" e terzietà, facenti capo all'Autorità per l'Informatica nella Pubblica Amministrazione, che certifica le loro chiavi⁴², gestisce l'elenco pub-

P.: in questo caso di P. K. I., ogni utente conserva la lista delle chiavi pubbliche degli altri utenti con cui si relaziona. La corrispondenza chiave-titolare è certificata dagli stessi, attraverso un sistema fiduciario incrociato (detto *web of trust*): se A certifica la corrispondenza B-chiave pubblica di B, ed allo stesso modo B la certifica per C, implicitamente A certifica anche C; ed, anzi, la "fiducia" può arrivare a far riconoscere ad A come valide anche tutte le associazioni chiave-titolare di B (non solo quindi quelle reciproche, ma anche quelle attuate con altri soggetti), e viceversa, fino alla creazione di una vera e propria "ragnatela" di certificazioni, a livello mondiale (così da JOHNSTON D., HANDA S., MORGAN C., *CyberLaw*, Stoddart Publishing, 1997, p. 100). È chiaro che un tale sistema mostra tutti i suoi limiti quando si cerchi di applicarlo non già ad una comunità non professionale e per fini relativi alla comunicazione personale (come nel caso della posta elettronica di Internet), ma per applicazioni più importanti, come ad esempio il commercio elettronico o i rapporti con la Pubblica Amministrazione. In particolare, non essendoci un modo diretto per revocare il certificato in caso sorgano problemi, né per verificare la vigenza della validità dello stesso, aumentando il numero degli utenti il sistema diventa impraticabile; poi, le informazioni contenute nel certificato del sistema P. G. P. non sono sufficienti, limitandosi in genere a permettere l'associazione chiave-indirizzo di posta elettronica; infine, è lo stesso modello di fiducia incrociata ad essere criticabile, e sicuramente non adatto per usi professionali (si pensi allo scambio di informazioni relative ad una controversia giudiziaria, in cui è il concetto stesso di fiducia ad essere discutibile).

⁴¹ Si vedano a tale proposito gli artt. 8 e 9, oltre all'art 1, lett. *b* e quelle da *m* a *p*, del Regolamento. Sul punto si veda anche il recente scritto di GRISOSTOMI TRAVAGLINI L., *La certificazione delle chiavi*, intervento al Convegno *I regolamenti di attuazione in materia di firma elettronica e archiviazione ottica dei documenti*, Roma, 25 e 26 novembre 1998, soprattutto con riferimento agli obblighi ed alle responsabilità del certificatore.

⁴² Definiti come quei soggetti, pubblici o privati, che effettuano la certificazione, ri-

blico in cui sono inserite e vigila relativamente alla presenza ed al mantenimento di specifici requisiti espressamente previsti dalla legge. Il DPCM 8 febbraio 1999 detta poi numerose norme che specificano le modalità con cui deve essere effettuata la procedura di certificazione, e disciplina quindi puntualmente la figura e le funzioni del certificatore. Questo mediante una serie di disposizioni che si riferiscono ai requisiti che deve avere per poter svolgere la relativa attività, alla sua organizzazione, alle modalità della sua attività (si veda ad esempio l'art. 16 sulla richiesta di iscrizione, l'art. 49 sull'organizzazione del personale del certificatore, l'art. 50 relativo ai requisiti di onorabilità, l'art. 24 che fissa l'obbligo di informazione nei confronti del richiedente il certificato e dei titolari degli stessi). Altra disciplina specificamente emanata per la regolamentazione dell'attività delle Autorità di certificazione, ultimo tassello per la completa realizzazione del sistema italiano di firma digitale, è la Circolare dell'A. I. P. A. 26 luglio 1999, n. AIPA/CR/22⁴³, che specificamente riporta le modalità attraverso le quali le società interessate ad esercitare l'attività di certificatore dovranno inoltrare domanda all'Autorità.

Uno dei compiti che il certificatore può svolgere è quello di validare temporalmente i documenti elettronici dei propri o di altri utenti: fattispecie che deve essere descritta, nonostante contribuisca ad aumentare la complessità del sistema, per la sua importanza in un contesto di circolazione automatica dei documenti.

2.3. La timbratura temporale

La validazione temporale, infatti, consiste nella generazione da parte di una terza parte fidata, normalmente una Autorità di certificazione, di un'ulteriore firma digitale aggiuntiva rispetto a quella del sottoscrittore, da cui si acquisisce la certezza circa il momento in cui questo è stato redatto ed è divenuto valido⁴⁴.

lasciano il certificato della chiave pubblica, lo rendono disponibile ai terzi unitamente a quest'ultima, pubblicano ed aggiornano gli elenchi dei certificati sospesi e revocati (così dall'art. 1, lett. m, del DPR 513), i certificatori in Italia hanno dunque struttura gerarchica verticale.

⁴³ In Gazz. Uff. 2 agosto 1999, Serie Generale, n. 179, e consultabile nel sito dell'Autorità, all'indirizzo <http://www.aipa.it> visitato il 1 settembre 1999.

⁴⁴ Definita nell'art. 1, lett. i, del D. P. R. 513 come "il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi", la sua disciplina è specificata nel Regolamento tecnico con un

Appare evidente l'utilità di tale procedura, fondamentale in tutte quelle fattispecie in cui risulta necessario acquisire una data certa per un determinato atto giuridico, come ad esempio per il perfezionamento della procedura di notificazione di atti processuali, oppure per individuare temporalmente una proposta contrattuale in modo da evitare possibili contestazioni, o ancora per dirimere ogni dubbio relativo al rispetto dei termini per la partecipazione ad una gara pubblica avvenuta attraverso l'invio dell'offerta attraverso la posta elettronica. Altra utilità della validazione temporale è la possibilità che questa realizza di garantire che un documento non venga in un secondo momento sostituito con uno diverso da parte dell'autore dello stesso, presentando per tale motivo analogie con l'autenticazione.

La procedura di marcatura temporale (anche detta di *time stamping*) si svolge attraverso i seguenti momenti:

- l'impronta del documento (calcolata, come si è detto, attraverso l'applicazione di una funzione di *hash* al messaggio) viene inviata al servizio di marcatura temporale, attuato per esempio da un certificatore⁴⁵;

- il servizio di marcatura aggiunge all'impronta ricevuta la data e l'ora, ottenendo una "impronta marcata";

- l'impronta marcata viene cifrata con la chiave segreta del soggetto che svolge il servizio, ottenendo la marca temporale da cui è possibile recuperare, mediante la sua chiave pubblica, l'impronta del documento e la data e l'ora della sua generazione;

- la marca temporale viene inviata al richiedente, il quale la allega al documento.

Descritta la procedura di validazione temporale, si procederà nella ora ad esporre una serie di possibili applicazioni di tale sistema.

3. Applicazioni pratiche del sistema di firma digitale

A fronte della complessità della costruzione legislativa, e delle non infrequenti incongruenze, il compito di ipotizzare una serie di applicazioni

intero titolo (il III) e nove diversi articoli (dall'art. 52 all'art. 60), e introducendo il concetto di "marca temporale", cioè l'evidenza informatica che consente la validazione temporale (art. 1, lett. f, del Reg. tecnico).

⁴⁵ L'impronta costituisce un riferimento certo al testo originale, ma allo stesso tempo non ne consente la ricostruzione: pertanto la marcatura può essere effettuata senza compromettere la confidenzialità dello stesso.

pratiche del sistema di firma digitale si rivela difficile e sottoposto al rischio di possibile smentita: si ritiene comunque utile procedere in questo modo per proporre argomenti che stimolino eventuali riflessioni, e magari aiutino nella comprensione della nuova procedura di imputazione dei documenti.

La prima ipotesi che si prende in considerazione riguarda le potenziali applicazioni della firma digitale nell'attività dell'avvocato.

3.1. *Nell'attività dell'Avvocato*

Con riferimento all'informatica giuridica l'Avvocatura, pur potendo usufruire delle positive novità apportate dalle tecnologie informatiche e telematiche per meglio svolgere la propria professione, ha troppo spesso assunto posizioni tendenzialmente distaccate da esse, se non addirittura nettamente avverse⁴⁶: rimanendo però in questo modo "tagliata fuori" dalla considerazione di coloro che dovevano decidere relativamente a tempi e direzioni dello sviluppo dell'informatica, oltre che in materia di investimenti per promuovere tale sviluppo⁴⁷. Nonostante ciò, le utilità connesse all'uso di informatica e telematica sono state finalmente comprese e sono quindi riuscite ad affermarsi presso l'indicata categoria: anche se in notevole ritardo, in maniera disorganica e non a livello culturale⁴⁸. Così, nell'ambito del processo di automazione degli uffici interessati all'amministrazione della giustizia, la maggior parte degli studi legali, in maniera diversamente capillare, si è dotata oggi di elaboratori elettro-

⁴⁶ Vantando il primato "del buon vecchio repertorio" sulle ricerche automatiche della documentazione giuridica nelle banche dati, su CD-ROM oppure *on-line*, o il piacere dell'uso della penna rispetto al digitare sulla tastiera, oltre a sottolineare la "competenza esclusiva" nell'uso dei computer della segretaria o dei giovani praticanti.

⁴⁷ Infatti oggi, a fronte di una quasi trentennale gestione da parte della magistratura e del Ministero di Grazia e Giustizia della documentazione giuridica in forma automatica (si pensi al sistema Italgire Find del C. E. D. della Corte di cassazione), e del recente avvio della rete intranet dei notai italiani (chiamata Rete Unitaria del Notariato, o R. U. N., che dopo pochi mesi dalla sua attivazione ha già collegato circa 1.000 notai su 4.500), rilevando che il sistema di firma digitale introdotto nel nostro Paese con il DPR 513 non proprio casualmente prevede compiti e funzioni per il solo notaio (si veda l'art. 16 e, almeno in parte, anche altre norme, come l'art. 7 comma I), deve segnalarsi l'assoluta mancanza di qualsiasi iniziativa simile, per importanza e diffusione, da parte degli avvocati.

⁴⁸ L'avvocato oggi "compra" e "usa" l'informatica e la telematica, ma senza preoccuparsi troppo di "conoscere" e "capire" entrambe.

nici e di programmi che gestiscono l'attività dell'avvocato. E sono state tentate anche alcune sperimentazioni⁴⁹, in particolare nel Foro di Roma, dalle vicende alterne: dalla possibilità di consultare i ruoli di Pretura, Tribunale e Corte d'Appello, all'avvio del sito web del Consiglio dell'Ordine, fino alla recentissima possibilità di conoscere l'importo da pagare all'ufficio del Registro Atti Giudiziari⁵⁰ per la registrazione dei provvedimenti giudiziari, iniziativa in collaborazione con il Ministero delle Finanze.

Tale situazione rende comunque ottimisti relativamente agli sviluppi futuri del settore, grazie all'entrata in vigore del sistema di firma digitale: e quindi, sulla base di alcuni presupposti accertati o prevedibili⁵¹, si ipotizzerà ora come potrebbe svolgersi l'attività dell'avvocato che finalmente vede riconosciuto dall'ordinamento pieno valore ai suoi documenti prodotti e gestiti mediante l'elaboratore.

3.1.1. *Il fascicolo elettronico*

Innanzitutto, in seguito alle novità legislative introdotte, si potrebbe gestire l'intero fascicolo relativo ad una determinata pratica direttamente in formato elettronico: chiaramente a fronte della parallela opera di in-

⁴⁹ In genere in conseguenza all'appassionata pressione di pochi, come nel caso dei colleghi Domenico Condello, Giorgio Palenzona e Giovanni Romano e degli altri partecipanti alla Commissione Informatica dell'Ordine degli avvocati di Roma, a cui si devono le iniziative indicate nel testo.

⁵⁰ In questo caso la sperimentazione è stata avviata anche per il Foro di Milano.

⁵¹ Nella specie, la considerazione che, alla luce di quanto appena affermato, ogni ufficio legale si può considerare dotato di una postazione informatica, e che quindi l'attività di documentazione dell'avvocato avvenga per la maggioranza in formato elettronico (come minimo la scrittura degli atti, ma probabilmente anche altre necessità del libero professionista, come la predisposizione delle parcelle, la gestione dello scadenziario e in genere dell'agenda legale, la tenuta delle scritture contabili, e magari anche l'archiviazione delle varie pratiche); e che una buona parte degli stessi sia anche munito (o stia per munirsi) di un collegamento ad Internet. Si può immaginare poi che in futuro il sistema di criptazione asimmetrica della classe forense venga gestito dallo stesso Ordine degli avvocati (in questo senso, tra l'altro, è anche il disposto dell'art. 17, comma IV, del DPR 513/1997). Sarà quindi questo organismo, a livello locale e nazionale, a coordinare l'acquisizione per i propri iscritti dei diversi apparati per sottoscrivere i documenti informatici, e dunque a svolgere il compito di Autorità di certificazione per la comunità forense, ed eventualmente anche quello di validazione temporale della documentazione automatica dei suoi utenti.

novazione che deve compiere anche l'ufficio giudiziario, di cui si parlerà nel prossimo paragrafo.

Già oggi, infatti, l'avvocato "lavora" due diversi formati di documentazione rispetto alla stessa pratica: da una parte quello digitale, per ora limitato all'eventuale risultato di ricerche in banche dati a diverso fine (per lo studio della pratica, e quindi nelle banche dati di legislazione-giurisprudenza-dottrina, oppure a fini probatori, come nel caso dei risultati delle visure camerali) ed all'atto scritto sul computer, ma in futuro esteso anche ad altri elementi utili per il procedimento (ad esempio un certificato di residenza oppure di destinazione urbanistica); dall'altra quello cartaceo, e dunque il fascicolo vero e proprio, composto della documentazione nata o acquisita come digitale e quindi successivamente stampata, e di quella invece su supporti tradizionali, per il momento in maggioranza rispetto alla prima. Ed in futuro potrebbe trasformare questo duplice formato, specchio della gestione ancora essenzialmente cartacea della sua attività, in uno unico, totalmente informatico: sia perché molti documenti, oggi in formato tradizionale, potrebbero già essere digitali *ab origine* (si pensi agli indicati certificati, o ad una fattura emessa direttamente in formato elettronico, magari mediante l'invio attraverso la posta elettronica), sia perché potrebbero essere resi tali, attraverso l'acquisizione della loro immagine con l'uso dello *scanner*.

In ogni caso il risultato sarebbe quello di un fascicolo totalmente elettronico, formato in tal modo, gestito in tal modo: anche nella fase più volte chiamata "dinamica", nella specie l'invio e il deposito presso l'ufficio giudiziario competente, la notificazione dell'atto di citazione o degli altri atti, la comunicazione con l'altra parte, il giudice e il proprio cliente. Il motivo per cui fino ad ora ciò non sia avvenuto deve ricercarsi principalmente nel mancato riconoscimento del documento elettronico nel nostro ordinamento, sia a livello di individuazione della sua natura, sia di accertamento del suo valore giuridico: rendendo così inaccettabile la gestione di un qualsiasi atto del procedimento attraverso i nuovi strumenti, e conseguentemente sempre necessaria la sua stampa. È chiaro che la situazione dovrebbe radicalmente cambiare, almeno teoricamente⁵², con l'adozione del sistema di firma digitale studiato nel presente scritto: vediamo come.

⁵² Una volta infatti messo in opera il sistema di firma digitale, ed accettata una riforma di quello tradizionale nel senso che si indica nel testo, occorrerà probabilmente attendere la sua esecuzione effettiva, dipendente dalla realizzazione dei presupposti indicati ad

Nella fase statica relativa alla formazione del fascicolo l'avvocato acquisirà i vari documenti della pratica inserendoli in un'apposita "cartella" (o *directory*) del proprio elaboratore elettronico, nella quale farà confluire anche gli atti scritti direttamente da lui. L'apposizione della sua firma digitale attraverso le modalità indicate in precedenza assicurerà il risultato di imputargli gli atti di cui è autore; per gli altri documenti invece, a seconda della specie di ognuno, avranno probabilmente già le loro firme digitali (ad esempio, una fattura elettronica allegata al fascicolo a fini probatori avrà apposta la sottoscrizione digitale di colui che l'ha emessa; un certificato sarà dotato di quella dell'ufficio pubblico che lo ha rilasciato). Nel caso invece voglia mantenere riservato l'intero fascicolo, a prescindere dunque da esigenze di autenticazione, applicherà allo stesso la sua chiave pubblica, crittografando l'intera cartella in modo che solo lui, con la propria chiave segreta, potrà decrittalarla e quindi leggere ed eventualmente modificare i singoli documenti che ne fanno parte (tranne chiaramente quelli che devono essere mantenuti nella loro versione originaria per finalità probatorie, come nel caso dei documenti appena indicati).

3.1.2. L'autentica

In tale fase assume fondamentale importanza il conferimento del mandato da parte del cliente.

Tradizionalmente questo viene concesso attraverso specifica procura in calce o a margine dell'atto di citazione, o della comparsa di risposta, sottoscritta dalla parte. Sottoscrizione che viene poi autenticata dallo stesso avvocato con l'apposizione della propria firma di seguito a quella del cliente, con la specificazione che è apposta "per autentica".

Le stesse modalità possono essere ripetute in formato elettronico grazie alla firma digitale.

In questo caso diventa inutile la distinzione relativa al punto dell'atto in cui viene inserito il mandato (in calce o a margine), essendo automatico (e comunque più facile) che ciò avvenga alla fine del documento, attraverso l'inserimento della stringa che è il risultato della crittazione mediante chiave privata dell'impronta della funzione di *hash*. A tale stringa verrà poi apposta la firma digitale dell'avvocato, per autentica, mediante una nuova cifratura della stessa, questa volta con la chiave privata del libero professionista.

Il giudice che volesse controllare l'esistenza e la validità del mandato, effettuerà le seguenti operazioni: prima applicherà la chiave pubblica del

legale procuratore della parte, ottenendo quindi il mandato cifrato da quest'ultima; applicherà allora la chiave pubblica della stessa parte, e poi la funzione di *hash*, riuscendo finalmente a leggere il testo originario: se il procedimento riesce senza difficoltà, e se il testo del mandato è adeguato, questo può essere ritenuto valido.

Occorre a questo punto specificare che quasi sicuramente la complessa procedura indicata verrà resa molto semplice per gli utenti (come si usa dire, "friendly") dai *software* di firma digitale⁵³: così, una volta espletate le formalità iniziali relative alla procedura di certificazione, l'attività del soggetto che firma, come quella del soggetto che vuole verificare un documento "firmato" (siano essi giudici, avvocati o pubblici amministratori), consisterà semplicemente nell'inserire la propria carta "intelligente" in un apposito lettore, che lavorerà poi insieme al *software* per la firma ed ai programmi di video scrittura o di gestione della posta per svolgere le indicate operazioni.

3.1.3. La comunicazione tra avvocati e la notificazione degli atti giudiziari

Chiaramente l'intera attività appena descritta può essere svolta non solo in presenza delle parti, ma anche a distanza, usando una rete telematica e specifici programmi di posta elettronica a tal fine. Ed essendo tale eventualità connaturata allo stesso sistema, non presenta particolari difficoltà.

Anzi è proprio la comunicazione (che necessariamente si deve instaurare tra il giudice e le parti, e tra le parti fra loro, per giungere ad una decisione corretta, all'accertamento della verità), e gli aspetti dell'attività dell'avvocato ad essa connessi, che risulteranno essere influenzati in maniera proficua dall'introduzione del sistema di firma digitale. Comunicazione che si esplica essenzialmente attraverso uno scambio di documenti, con finalità diverse: talvolta nell'ambito dell'attività delle parti stesse, senza rilevanza esterna e senza bisogno di alcuna garanzia circa lo svolgimento di tale comunicazione; altre volte nel corso di un preciso

inizio paragrafo, e quindi dalla predisposizione degli uffici giudiziari e dei loro addetti in tal senso.

⁵³ Anzi, molto probabilmente tale requisito, la semplicità d'uso, sarà uno dei punti fondamentali per la riuscita dell'intero progetto, insieme, certamente, all'investimento in cultura delle nuove tecnologie.

momento del procedimento, preso in considerazione dal legislatore che richiede la certezza dell'avvenuta attività di trasmissione del documento.

I problemi sollevati dalle due ipotesi considerate sono quindi diversi. Nel primo caso non assume rilevanza il procedimento di comunicazione, che si svolge tra le parti, ma il risultato di tale attività, cioè il documento stesso che si produce⁵⁴; e quindi anche in passato non si sono avute grandi difficoltà a riconoscere valide modalità alternative all'uso della carta ed ai mezzi tradizionali di trasmissione di questa (essenzialmente il servizio postale), purché il risultato fosse di per sé valido: così ad esempio si ammise l'uso del *telex*, inizialmente ad opera dell'interpretazione particolarmente evolutiva della giurisprudenza, poi attraverso una specifica produzione legislativa in tal senso⁵⁵. Difficoltà si ebbero chiaramente ad andare oltre, e quindi ad ammettere una gestione interamente digitale dell'indicata attività, per i noti problemi legati al mancato riconoscimento dei documenti informatici.

Nella seconda ipotesi, invece, è proprio la trasmissione degli atti ad essere presa in considerazione dalla legge, che la disciplina costruendola in modo tale da permettere di raggiungere la certezza circa l'avvenuta comunicazione di un determinato documento ad una determinata persona. Questo mediante una procedura apposita, detta di notificazione,

⁵⁴ Le difficoltà riguardano, ad esempio, il valore da attribuirsi a tale documento quando non sia l'originale (come nel caso di atto trasmesso attraverso *telex*). Si immagini in particolare l'ipotesi di una procura conferita ad un avvocato dalla parte attraverso l'invio del mandato sottoscritto mediante il *fax*: il giudice dovrà decidere in quale modo valutare tale documento prodotto dalla parte, se attribuirgli o meno validità, e che valore probatorio conferirgli.

⁵⁵ Ci si riferisce alla legge 7 giugno 1993, n. 183, che ha reso possibile la trasmissione per mezzo del computer e della telematica (la norma parla genericamente di "mezzi di telecomunicazione") di copia degli atti o dei provvedimenti del processo ad altro avvocato, copia che si considera conforme all'originale se entrambi i legali siano muniti di procura ex art. 83 del codice di procedura civile (procura che può risultare anche dall'atto trasmesso), l'atto sia sottoscritto in maniera leggibile da parte dell'avvocato trasmittente, la copia ricevuta sia sottoscritta per la conferma dal ricevente. Nel caso ricorra quest'ultimo requisito, si considera conforme all'originale anche la copia teletrasmessa di atti o provvedimenti relativi ad altri processi. La disciplina stabilita in tale legge permette ad esempio ad un avvocato che debba notificare, ovvero depositare in cancelleria, un atto in un luogo diverso da quello della sua residenza, di avvalersi della collaborazione di un collega che effettui tale operazione sul posto in cui gli atti sono diretti, trasmettendo a quest'ultimo gli atti stessi mediante *telex* invece che attraverso il servizio postale. Il secondo legale provvederà poi ad utilizzare gli atti ricevuti, notificandoli o depositandoli, grazie al valore di copia conforme all'originale attribuita loro dalla normativa in esame.

svolta da un ausiliario del giudice, l'ufficiale giudiziario, che permette di ritenere pienamente provata l'attività di comunicazione effettuata. In tale caso la posizione nei confronti di modalità alternative di svolgimento dell'indicata attività era di netta chiusura: non solo relativamente ai mezzi impiegati, che dovevano essere necessariamente quelli tradizionali (l'atto cartaceo da notificare, l'attività dell'ufficiale giudiziario che si recava presso il domicilio del destinatario, la sottoscrizione di questo sulla copia dell'atto, la relata di notifica), ma anche ai soggetti necessariamente coinvolti (in particolare proprio l'ufficiale giudiziario). Anche su tale sistema intervenne il legislatore con apposita disciplina, la l. 1 luglio 1994 n. 53, relativa alla notificazione di atti da parte degli avvocati, introducendo due nuove possibilità, oltre a quelle già previste dal codice di procedura: Secondo la prima ipotesi, disciplinata dall'art. 1 della stessa legge, diventava possibile per gli avvocati effettuare direttamente ogni notifica a mezzo del servizio postale; il secondo tipo di notificazione introdotto riguarda invece gli avvocati domiciliatari delle parti nei relativi procedimenti, ipotesi in cui, soddisfatte alcune formalità richieste dall'art. 4 della legge in esame, è possibile procedere alla notificazione direttamente, mediante consegna di copia dell'atto nel domicilio del destinatario. In entrambi i casi veniva meno la necessità della presenza dell'ufficiale giudiziario: l'avvocato o procuratore che svolge tale attività, infatti, viene considerato pubblico ufficiale ad ogni effetto (art. 6), conferendo quindi valore di piena prova alle dichiarazioni effettuate in relazione all'attività svolta.

Circa i mezzi utilizzabili, la legge espressamente parla di notificazioni "a mezzo del servizio postale" (art. 1) nel caso della prima ipotesi, e di "consegna di copia dell'atto nel domicilio del destinatario" (art. 4) nella seconda ipotesi. La dizione testuale della legge permetteva all'interprete di far rientrare, in entrambi i casi, nella previsione astratta della normativa in esame, l'utilizzo dei nuovi sistemi informatici e telematici: per quanto riguarda la prima ipotesi, l'adozione delle forme più moderne di "servizio postale", quali la posta elettronica; per quanto riguarda la seconda ipotesi, un qualsiasi mezzo informatico o telematico (in genere sempre quelli di comunicazione elettronica via *modem*) che permetta la "consegna" (termine che deve essere inteso in senso ampio, tenendo presente il risultato da ottenere, e non il mezzo utilizzabile) di copia del documento⁵⁶.

⁵⁶ Ci si poteva poi riferire alla già ricordata legge 183/1993 per ricavare il valore giuridico del documento inviato tramite i nuovi mezzi ("copia conforme all'originale").

In entrambi i casi l'introduzione di un articolato sistema come quello della firma digitale ha portato rilevanti novità a sostegno delle prime interpretazioni dottrinarie⁵⁷. Innanzitutto per le nuove figure immesse nel sistema, fin dal momento della loro definizione o per il fatto di essere state considerate a livello legislativo: ci si riferisce in particolare ai concetti di "indirizzo elettronico", di "trasmissione del documento informatico" e di "validazione temporale". Poi perché viene espressamente prevista una norma, l'art. 12 del DPR 513, che non solo conferisce piena dignità giuridica al servizio della posta elettronica, attraverso il riconoscimento dell'indirizzo elettronico come recapito valido per inviare, e considerare pervenuti, documenti informatici; ma nel suo terzo comma introduce anche una "rivoluzionaria" disposizione che equipara la trasmissione del documento informatico per via telematica (con modalità che assicurino l'avvenuta consegna) alla notificazione per mezzo della posta tradizionale. Infine perché, in generale, conferisce un valore giuridico al documento informatico, e quindi risolve parte delle difficoltà incontrate dalle due leggi citate.

Così, nel momento in cui l'intero nuovo sistema diventerà effettivamente operativo, sarà possibile realizzare comunicazioni e notificazioni di atti processuali in forma elettronica.

Nel caso delle comunicazioni, grazie al nuovo valore giuridico che acquisisce il documento informatico: così, alla ricordata libertà di forme nello svolgimento dell'attività comunicativa, che si svolge tra le parti, già accettata in precedenza, si aggiunge la possibilità di accogliere il risultato di tale attività, cioè il documento stesso che si produce, direttamente in formato elettronico senza la necessità di avere la sua stampa. Allora, nell'esempio fatto, l'avvocato che volesse avviare una pratica in altro Foro rispetto a quello di appartenenza, non avrebbe più bisogno del collega che lo assista svolgendo un'attività di mero recettore dei suoi atti e di "strumento" per la loro resa cartacea⁵⁸ e consegna in tale forma all'uffi-

⁵⁷ Si veda a tale proposito CIACCI G. - VARI P., *Forme alternative di notificazione: la notifica mediante strumenti informatici*, in *Rivista di Diritto Commerciale*, Padova, 1994, 1/2, pp. 95-132; COSTANTINO G., *Sulla trasmissione di atti processuali attraverso mezzi di telecomunicazione (prime note sulla legge 7 giugno 1993 n. 183)*, in *Il Foro Italiano*, 1993, I, p. 2500; BORRUSO R., *L'uso processuale del fax*, in *Informatica e documentazione*, 1993, p. 15, ancora CIACCI G., *Comunicazioni e notificazioni di atti processuali in forma elettronica*, in *La tecnologia dell'informazione e della comunicazione in Italia. Rapporto FTI 1996*, FrancoAngeli, Milano, 1997, p. 262-282.

⁵⁸ E conseguentemente per il conferimento allo stesso di un valore giuridico: si pensi

cio giudiziario: potrebbe invece direttamente depositare il ricorso in via telematica presso l'ufficio giudiziario competente, anche se lontano dal distretto in cui esercita.

Nel caso invece delle notificazioni, è proprio l'art. 12 del DPR 513 citato a conferire alla prima modalità introdotta dalla l. 53/1994, notificazione diretta di atti da parte degli avvocati "a mezzo del servizio postale", la possibilità di assumere una "veste" elettronica, e quindi di essere effettuata a mezzo del servizio postale elettronico. La condizione in quest'ultimo caso è che vengano adottate modalità che "assicurino l'avvenuta consegna", ma questo risultato è connaturato allo stesso sistema: da una parte grazie alla modalità propria della crittografia asimmetrica, che permette di ottenere la sicurezza relativa alla provenienza, non ripudiabilità e genuinità del documento informatico (l'atto di citazione in appello gestito in formato elettronico e notificato in via telematica); dall'altra la procedura di validazione temporale⁵⁹, che permette di essere certi della data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, risultato essenziale per il procedimento di notificazione richiesto dalla legge. In pratica si può pensare ad un sistema organizzato proprio con l'intermediazione dell'Ordine degli avvocati a cui appartengano i due legali che effettuano l'indicato procedimento, che come si è detto probabilmente assumerà i compiti di Autorità di certificazione per la classe forense, svolgendo anche l'attività di validazione temporale dei documenti informatici degli stessi: l'avvocato quindi che volesse inviare via posta elettronica un documento ad altro avvocato a fini di notificazione dello stesso, lo farà passando attraverso il filtro dell'Ordine che, associando una marca temporale all'atto "in transito" attraverso il suo sistema, renderà opponibili ai terzi la data e l'ora di formazione, di trasmissione o di ricezione dello stesso.

Certamente un sistema ancora da organizzare correttamente, non solo nella sua concezione teorica, al di là delle affermazioni troppo generiche del DPR 513 e del silenzio del suo regolamento tecnico, ma anche nella sua attuazione pratica, tra l'altro con la predisposizione tecnica degli uffici sia dei vari Consigli dell'Ordine dei diversi distretti (a meno di cen-

all'atto inviato via *telefax*, a cui il legale destinatario appone la sua firma per renderlo valido, anzi "copia conforme all'originale" ai sensi della l. 183/1993.

⁵⁹ Che ricordiamo viene definita nell'art. 1, lett. *i*, del DPR 513 come "il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi".

tralizzare le funzioni nel Consiglio Nazionale Forense), sia degli Uffici giudiziari e degli Uffici Notifiche. In questo caso però, una volta reso effettivamente operativo, le utilità che ne potrebbero derivare saranno molto importanti, permettendo l'ottimizzazione delle procedure di comunicazione tra i vari soggetti che svolgono la loro attività nel "pianeta-Giustizia", attraverso l'informatica e la telematica, e contribuendo concretamente a risolvere i problemi connessi alla disastrosa situazione in cui versa il processo nel nostro Paese. Dopo di che l'iniziativa passerebbe agli indicati soggetti, ed in primo luogo agli avvocati, che, vincendo resistenze mentali e radicati atteggiamenti di diffidenza nei confronti dei nuovi strumenti, devono procedere ad un maggiore uso consapevole delle tecnologie informatiche e telematiche nella loro attività. A vantaggio di tutti.

3.1.4. *Il deposito di atti giudiziari*

Dopo l'avvenuta notifica del proprio atto alla parte avversa, l'avvocato dovrà depositare il fascicolo relativo alla pratica presso l'ufficio giudiziario competente. Fascicolo che ricordiamo è gestito dal libero professionista in forma elettronica, e che quindi deve essere mantenuto tale anche una volta avviato il vero e proprio procedimento.

Così, anche l'ufficio giudiziario dovrà essere automatizzato, anche se tra l'altro l'ipotesi della "cancelleria informatica" non è poi così lontana dalla realtà, non tanto sulla base dell'esperienza quotidiana del libero professionista⁶⁰, quanto su altri, meno visibili, situazioni: ad esempio, già oggi l'iscrizione a ruolo di una causa presso la cancelleria viene effettuata attraverso la compilazione di un modulo, da allegare al fascicolo cartaceo, la nota di iscrizione a ruolo, ricco di cifre e numeri, che poi serve per la registrazione elettronica dello stesso; grazie a tale registrazione è possibile seguire la "vita" del procedimento, attraverso la consultazione dell'archivio dei ruoli, oggi già tenuto in maniera informatica e, per alcuni distretti, anche a distanza attraverso un collegamento telematico; spesso poi gli stessi giudici scrivono direttamente i propri provvedimenti direttamente al computer, e quindi sarebbero teoricamente già disponibili in

⁶⁰ Abituato a vivere l'attività di udienza come un caotico momento pieno di carta, di fascicoli archiviati in disordinati faldoni spesso difficili da trovare, sottoposti a frequenti e talvolta mirate "sparizioni", con computer spenti sui tavoli dei giudici, magari utilizzati come deposito momentaneo di documenti o codici.

formato elettronico. Sono quindi in atto diverse sperimentazioni di diverse fasi del procedimento, che potrebbero poi confluire nella gestione del "fascicolo elettronico" da parte anche dello stesso ufficio giudiziario.

Il nuovo valore giuridico acquisito dal documento elettronico e dalla trasmissione telematica dello stesso, grazie alla crittografia a chiavi asimmetriche ed alla firma digitale, conferirebbe all'intero sistema un nuovo fondamento ed un nuovo impulso, grazie all'acquisita certezza delle varie operazioni che si andrebbero a compiere attraverso l'informatica: oltre al deposito elettronico del fascicolo (grazie all'art. 12 del DPR 513), si pensi al rilascio delle copie dei vari atti (ex art. 6 DPR 513), alla conservazione degli stessi (ancora art. 6 e art. 15, oltre alla nuova Deliberazione A. I. P. A. 30 luglio 1998, n. 24/98, sulle "Regole tecniche per l'uso di supporti ottici"), ai pagamenti elettronici delle varie marche e tasse (art. 14 DPR 513).

Ottenuti, finalmente, gli strumenti opportuni da parte del Legislatore, come si è detto spetterà direttamente agli operatori del diritto, una volta resi operativi, concretamente procedere ad utilizzarli, decretandone il successo o il fallimento. L'ottimismo è diretta conseguenza da una parte della consapevolezza dell'utilità dei nuovi strumenti per migliorare il lavoro degli stessi operatori, dall'altra dei buoni risultati che stanno ottenendo le prime sperimentazioni di automazione di alcune procedure già in corso da diverso tempo.

3.1.5. *La sperimentazione in atto sulla consultazione automatica dei Ruoli e delle funzioni connesse con la liquidazione e registrazione di atti giudiziari*

Con un'autorizzazione fornita su richiesta agli avvocati del Foro di Roma, è possibile da circa tre anni consultare, in tempo reale per via telematica dal proprio studio⁶¹, i Ruoli Generali civili della Corte d'Appello, del Tribunale e della Pretura⁶², ed in particolare i procedimenti in cui è costituito. L'adesione al sistema è stata entusiasta, circa 3.000 avvocati li consultano con continuità, a dimostrazione del fatto che, quando

⁶¹ La consultazione direttamente presso gli uffici giudiziari attraverso terminale invece del registro cartaceo era già possibile da diversi anni.

⁶² Come è noto il Ruolo è un registro tenuto dalla cancelleria dello specifico ufficio giudiziario, nel quale vengono iscritti tutti i procedimenti giudiziari pendenti nello stesso ufficio, con le informazioni relative alle parti, all'oggetto della causa, al giudice, ai rinvii ed ai provvedimenti pronunciati.

viene introdotto un servizio utile e di non eccessiva difficoltà, il successo è garantito anche se l'utente non è dotato di una grande familiarità con i nuovi strumenti. Simili sperimentazioni sono poi state avviate anche in altri Consigli dell'Ordine: si segnala a tale proposito l'iniziativa della comunità forense di Patti per i ruoli del Tribunale e della Pretura della stessa città; oltre a quelli delle Preture di S. Agata Militello e di S. Angelo di Brolo, che, nonostante si riferisca ad una realtà di limitate dimensioni, si caratterizza per essere disponibile non già attraverso un collegamento telematico diretto (come avviene per Roma), ma su Internet⁶³.

Il sistema della firma digitale, in questo caso, non influirà tanto sulle modalità di svolgimento di questa attività, che rimarrà sostanzialmente immutata⁶⁴, quanto su operazioni ulteriori che saranno rese possibili: come ad esempio la possibilità di stampare direttamente sul proprio computer copia del provvedimento del giudice con il valore dell'originale (si veda il già citato art. 6 del DPR 513), con la sicurezza della sua provenienza e genuinità.

Altra sperimentazione che deve essere considerata, avviata per lo snellimento delle attività connesse alla registrazione dei provvedimenti giudiziari (sentenze, decreti ingiuntivi, esecuzioni immobiliari, ecc.), riguarda la realizzazione presso l'Ufficio del Registro di Roma e quello di Milano Atti Giudiziari (ma alla fine di un primo periodo di prova il servizio verrà esteso a tutto il territorio nazionale), di una procedura che prevede da una parte l'acquisizione dei dati per la tassazione dei provvedimenti giudiziari da parte dell'ufficio, dall'altra l'inserimento nel sito Internet del Ministero Finanze degli importi da pagare per la registrazione. Per richiedere le informazioni sulle tasse da pagare per la registrazione di un provvedimento l'utente interessato, in genere uno degli avvocati delle parti, si collega col sito Internet del Ministero⁶⁵ e inserisce gli estremi del provvedimento che deve registrare in un'apposita *form* che poi provvederà ad inviare seguendo le istruzioni in esso contenute. Le informa-

⁶³ L'indirizzo del sito web che ospita l'iniziativa è <http://www.legacy.it/forrpatti/or-davv.htm> consultato il 5 gennaio 1999.

⁶⁴ Probabilmente, a fronte dell'aumento degli utenti dello stesso, una volta diffuso maggiormente l'uso della telematica grazie magari ad altre applicazioni, non necessariamente professionali (si pensi ai servizi di Internet), anche la sua qualità aumenterà: magari con una maggiore velocità di consultazione, o relativamente alla quantità di informazioni acquisibili, o ancora sulle modalità di ricerca dei dati.

⁶⁵ E specificamente alla pagina dedicata al servizio, all'indirizzo <http://www.finanze.interbusiness.it/avvocati> consultato il 5 settembre 1999.

zioni fornite in risposta si riferiscono, tra l'altro, al codice dell'ufficio dove viene effettuata la registrazione, la causale del versamento, gli estremi dell'atto, i codici dei tributi da pagare, gli importi dei singoli tributi e l'importo totale da versare.

Una volta acquisite queste informazioni l'interessato dovrà comunque provvedere al pagamento recandosi poi direttamente all'Ufficio del Registro, ma in questo modo eliminerà un passaggio causa spesso di inutili perdite di tempo. Non è infatti ancora prevista la possibilità di pagare direttamente su Internet la registrazione dei provvedimenti⁶⁶: questo sia per l'attuale insicurezza delle transazioni elettroniche attraverso la Rete, sia perché non è ancora riconosciuta dall'ordinamento il fondamento giuridico di questa forma di trasferimento elettronico dei fondi. In questo caso l'introduzione di un sistema di firma digitale, ed in particolare la concreta attuazione della disciplina del DPR 513 (nella specie il suo art. 14 relativo ai pagamenti informatici), permetterebbe di superare le indicate difficoltà, e potrebbe servire da stimolo alla nascita di nuove concrete iniziative volte a semplificare e velocizzare l'attività dell'avvocato.

3.2. Nell'attività del Notaio

Prendiamo ora in considerazione l'attività di un altro libero professionista che è direttamente interessato dalla recente innovazione in materia di documentazione automatica, il notaio.

In questo caso occorre subito evidenziare alcuni aspetti peculiari di tale figura: da una parte perché la posizione del notaio nei confronti dell'informatica è totalmente diversa rispetto alla classe forense; dall'altra perché è lo stesso DPR 513 a prendere in considerazione la figura del notaio, stabilendo per lui alcune funzioni specifiche anche nel nuovo sistema. Dal primo punto di vista, l'approccio nei confronti delle nuove tecnologie, i notai sono sempre stati molto aperti verso l'innovazione, che permetteva loro di svolgere le proprie funzioni in maniera più efficiente ed adeguata alle rinnovate esigenze di assicurare garanzie di certezza nel momento in cui i traffici giuridici avevano assunto la velocità conseguente all'uso dei nuovi strumenti; ed in tale ottica ha visto recentemente la luce la Rete Unitaria del Notariato che, dopo soli pochi mesi dalla sua attivazione ha già collegato circa 1.000 notai su 4.500⁶⁷.

⁶⁶ Anche se sono in avanzata fase di studio alcune attuazioni in collaborazione con un importante istituto bancario

⁶⁷ Per avere notizie aggiornate su tale Rete si può consultare il sito web del Consi-

Dal secondo punto di vista, e cioè la considerazione della figura del notaio da parte del DPR 513, si devono ricordare: l'art. 6, comma III, che rende necessaria la sua attestazione della conformità all'originale delle copie su supporto informatico di documenti, formati in origine su supporto cartaceo (o, comunque, non informatico), se si vuole che queste ultime sostituiscano, ad ogni effetto di legge, gli originali da cui sono tratte; l'art. 7, in materia di deposito, in forma segreta, della chiave privata di un soggetto, che può essere effettuato "presso un notaio o altro pubblico depositario autorizzato"; ed infine l'art. 16, in materia di firme digitali autenticate⁶⁸.

Il sistema della firma digitale, quindi, crea per il notaio una nuova serie di attività⁶⁹, oltre a permettere di dare fondamento giuridico a quelle che già in passato venivano gestite attraverso l'uso dell'elaboratore elettronico. Per meglio comprendere come poi in pratica avvenga l'influenza del nuovo sistema su entrambi i tipi di attività, si ritiene utile riportare un esempio relativo al ricevimento di un atto pubblico da parte del notaio⁷⁰, con le modalità stabilite nel DPR 513.

Anche in questo caso si deve partire dal presupposto che il pubblico ufficiale sia dotato dell'apparecchiatura necessaria alla stipulazione con modalità informatiche, e che quindi sia anche munito del software adatto e delle chiavi di crittografia asimmetrica, di cui quella pubblica certificata e pubblicata presso l'Autorità di certificazione competente per la sua categoria professionale. La prima operazione che compirà sarà l'identificazione delle parti mediante la procedura tradizionale, a cui si dovrà aggiungere l'accertamento dell'identità informatica delle stesse⁷¹, attraverso

glio Nazionale del Notariato, all'indirizzo <http://www.notariato.it> consultato il 15 gennaio 1999. Si veda anche MACCARONE E., nella sua Relazione al Congresso Nazionale del Notariato tenuto a Roma il 29 novembre 1997.

⁶⁸ Relativamente a tale articolo, che ha suscitato diverse polemiche tra gli studiosi della materia, ma anche per gli altri due, si veda quanto diffusamente esposto in sede di commento al DPR 513, in CIACCI G., *La firma digitale*, cit., p. 133.

⁶⁹ Si è parlato, a tale proposito, di una nuova figura di notaio, il "Cybernotary", in seguito all'accresciuta rilevanza che tale professionista dovrebbe ottenere in una realtà sovranazionale di cui il commercio elettronico è parte (così BARRESI R. G., *Aspetti comparatistici del notariato fra Italia e Inghilterra*, in *Vita notarile*, ottobre 1998, e MICCOLI M., *Cybernotary*, in *Notariato*, 1996, p. 107.

⁷⁰ Così anche MICCOLI M., *Documento e commercio telematico*, IPSOA, Milano, 1998, p. 108.

⁷¹ In tal senso ANDRINI M. C., *Dal tabellone al significato elettronico*, relazione al Convegno "Cyberlaw", Roma, 9 luglio 1998, p. 6.

questa volta una nuova modalità: in particolare, egli dovrà verificare la corrispondenza dispositivo di firma – titolare, e quindi constatare la validità della chiave pubblica della parte, e del relativo certificato⁷². A questo punto il notaio indagherà personalmente la volontà delle parti e, effettuate le verifiche preliminari richieste dalla legge o dalla natura dell'atto (molte delle quali, nel momento di attuazione della riforma della P. A. che coinvolgerà una sua maggiore automazione, in via telematica: si pensi ad esempio, le visure catastali o ipotecarie fatte nei Registri immobiliari informatizzati), redigerà lo stesso direttamente su supporto informatico, utilizzando il proprio elaboratore elettronico. Secondo la prescrizione dell'art. 51 n. 8 della legge notarile, leggerà l'atto così redatto alle parti, apportandovi eventualmente le opportune modifiche per renderlo esattamente conforme alla volontà delle stesse; in questa fase il formato elettronico probabilmente renderà inutili le "postille", essendo possibile correggere direttamente il testo, almeno fino all'apposizione della firma elettronica delle parti, momento in cui l'atto assumerà la veste definitiva⁷³. La sottoscrizione dell'atto avverrà con le nuove modalità: così il notaio chiederà a ciascuna delle parti di apporre in calce all'atto, in sua presenza, la loro firma digitale, utilizzando la funzione di *hash* e la loro chiave privata all'impronta da questa risultante (nei modi già più volte ricordati), di seguito alla quali apporrà poi la propria firma digitale.

Il documento che ne risulterà sarà un testo crittografato, che potrà essere reso leggibile con l'utilizzo della chiave pubblica del notaio sull'impronta di *hash*⁷⁴ del documento stesso, dal quale sarà poi possibile

⁷² Il notaio, per verificare la validità dell'apparato tecnico usato dalla parte per firmare il documento informatico, prima potrebbe farlo usare, cioè fare usare sul documento informatico la chiave privata della parte; quindi, applicata la chiave pubblica della stessa, certificata (da cui risultassero i dati identificativi del titolare, e la durata della validità della chiave e del relativo certificato, che il notaio dovrebbe verificare collegandosi al sito del certificatore del soggetto), per "aprire" il documento "firmato"; in caso il procedimento riuscisse, il notaio sarebbe dunque sicuro della validità di tale apparato. Altra più semplice modalità sarà invece connessa all'uso del dispositivo di firma: il notaio identifica la parte con i mezzi tradizionali, quindi verifica la titolarità del dispositivo di firma da questo usato, e la correttezza del P. I. N. necessario per attivarlo (e questo sarà sufficiente per accertare la sua legittimazione all'uso della chiave privata); controllerà poi la validità della chiave pubblica, attraverso il certificato del soggetto.

⁷³ Così ANDRINI M. C., op. cit., p. 2.

⁷⁴ Ci si riferisce al documento sottoscritto con la tecnica della crittografia asimmetrica e della funzione di *hash*, con testo visibile in chiaro, e quindi non interamente cifrato.

identificare con certezza sia il pubblico ufficiale che l'ha ricevuto, sia la sua competenza; applicando, dunque, la chiave pubblica di ciascuna delle parti alle rispettive impronte, se ne trarranno informazioni coincidenti con quelle risultanti dall'atto decrittato. A questo punto, reso definitivo l'atto, saranno possibili le eventuali correzioni attraverso le postille, che avverranno in questo caso associando al documento elettronico principale un documento elettronico accessorio, munito ancora delle firme digitali di parti e notaio⁷⁵.

Concluso il momento di ricevimento dell'atto, il notaio passerà ad adempiere alle successive incombenze. E quindi, innanzitutto, quella relativa al repertorio che, sulla base del presupposto della gestione informatizzata della sua attività, sarà tenuto su supporto informatico ai sensi dell'art. 15 del Regolamento, supporto che dovrà avere caratteristiche di non riscrivibilità e di inalterabilità, quali quelle oggi offerte dai dischi ottici, nella loro formula *WORM*⁷⁶. Il notaio redigerà le copie dell'atto, sempre in maniera informatica, ai sensi dell'art. 6 del Regolamento, apponendo quindi alle stesse la propria firma digitale di seguito alla formula di conformità. Anche la trasmissione delle copie ai pubblici uffici avverrà nell'ambito di una gestione informatizzata degli stessi, in una fase di pieno compimento ed attuazione della Rete Unitaria della Pubblica Amministrazione da una parte (grazie alla quale tutti gli uffici dell'amministrazione saranno collegati tra di loro e accessibili dall'esterno da parte di professionisti o semplici cittadini), e di quella del notariato dall'altra: si potrà quindi trasmettere attraverso posta elettronica sicura le copie autentiche di documenti informatici, ed in particolare basterà inviarne una sola ad un unico ufficio perché possano con ciò ritenersi adempiute le formalità di registrazione, trascrizione e voltura dell'atto. Parallelamente dovranno essere pagate anche le imposte, i diritti e i tributi afferenti il negozio, anche in questo caso attraverso modalità telematiche, che si saranno sviluppate sulla base dell'art. 14 del DPR 513. Il notaio sarà infine esonerato dall'esibizione dell'originale, grazie al comma III dell'articolo 6 dello stesso DPR.

3.3. Nell'attività del commercialista

Per quanto riguarda l'attività dell'ultimo libero professionista che si

⁷⁵ Ancora ANDRINI M. C., cit., p. 2.

⁷⁶ Dischi ottici che è possibile incidere una sola volta, e non più modificare, mentre sarà poi possibile leggerli molte volte (*Write Once, Read Many*).

prenderà in considerazione in questo paragrafo dedicato alle ipotesi di applicazione pratica del sistema della firma digitale, il commercialista, valgono i rilievi già esposti per gli altri due. In questo caso però, a parte l'influenza relativa alla sua attività che già si svolgeva attraverso l'uso dell'elaboratore elettronico per la formazione e conservazione della propria documentazione, comune a quella degli altri due professionisti esaminati (e quindi l'acquisito valore giuridico di tale attività), deve essere esaminata una originale iniziativa introdotta di recente nel nostro ordinamento, ed ora in piena fase di realizzazione.

Ci si riferisce alla possibilità, per il commercialista e per una serie di altri soggetti (altro libero professionista, CAAF e associazione di categoria), di presentare le dichiarazioni dei redditi dei propri clienti attraverso sistemi telematici⁷⁷, introdotta dal decreto legislativo 241/1997 e disciplinata con diverse finalità attraverso una serie di altre norme⁷⁸; mentre le società ed enti di rilevante dimensione (capitale sociale o patrimonio netto superiore a 5 miliardi) dovranno presentare direttamente le proprie dichiarazioni utilizzando anch'esse il servizio telematico predisposto dall'Amministrazione. Tutti coloro che utilizzano il servizio devono essere previamente autorizzati, mediante la presentazione alla Direzioni Regionali delle Entrate o alle Direzione delle Entrate territorialmente competente, di un'apposita "Domanda di abilitazione": domanda che deve essere presentata entro termini precisi, fissati a seconda della singola ca-

⁷⁷ I contribuenti che non si avvalgono di un intermediario possono presentare la propria dichiarazione ad una banca convenzionata con l'Amministrazione finanziaria, oppure direttamente agli uffici postali, che provvedono all'acquisizione dei dati e alla loro trasmissione, sempre però in via telematica, alla stessa Amministrazione.

⁷⁸ Nella specie il DPR 22 luglio 1998 n. 322, contenente il "Regolamento recante modalità per la presentazione delle dichiarazioni relative alle imposte sui redditi, all'imposta regionale sulle attività produttive e all'imposta sul valore aggiunto, ai sensi dell'articolo 3, comma 136, della legge 23 dicembre 1996, n. 662"; il Decreto dirigenziale del 31 luglio 1998, decreto emanato ai sensi dell'articolo 12, comma 11, del decreto del Presidente della Repubblica 29 settembre 1973, n. 600, e concernente modalità tecniche di trasmissione telematica delle dichiarazioni; il Decreto dirigenziale del 17 settembre 1998 che detta "Criteri per l'individuazione dei soggetti incaricati della trasmissione telematica delle dichiarazioni in materia di imposte sui redditi, I. R. A. P. e I. V. A. ". Nella fase esecutiva di tale modalità, numerosi sono stati gli interventi correttivi da parte del Ministero, tra cui ricordiamo i recenti DPCM 17 settembre 1999, sul differimento dei termini per l'invio elettronico delle dichiarazioni, e la Circolare 195/E contenenti chiarimenti per la trasmissione telematica. Questi e altri provvedimenti sono consultabili direttamente nel sito del Ministero delle Finanze, all'indirizzo <http://www.finanze.it>.

tegoria di intermediari. Comunque, a prescindere dal momento in cui viene richiesta l'abilitazione al servizio, con il 1 gennaio 1999 sono unificate tutte le dichiarazioni, e razionalizzate le modalità di presentazione, prevedendo unicamente: la presentazione diretta da parte del contribuente del modello cartaceo compilato alle banche e agli uffici postali e agli intermediari autorizzati (su tutti chiaramente il commercialista), che provvederanno all'acquisizione dei dati e alla loro trasmissione in via telematica all'Amministrazione finanziaria; la presentazione in via telematica delle dichiarazioni da parte delle società ed enti di rilevante dimensione; la presentazione in via telematica delle dichiarazioni predisposte, su incarico dei contribuenti, da parte di alcune categorie di soggetti (professionisti, associazioni di categoria e Centri Autorizzati di assistenza fiscale) individuati dall'art. 12 del D. P. R. n. 600/73.

Notevoli i vantaggi acquisiti, sia per l'Amministrazione finanziaria, sia per il contribuente: per quanto riguarda il primo punto di vista, la presentazione della dichiarazione con i nuovi strumenti ha permesso di acquisire, senza alcuna lavorazione di tipo manuale e nel giro di pochi mesi, dati e informazioni che in precedenza pervenivano dopo anni; e quindi innanzitutto vantaggi in termini di tempestività nella disponibilità delle informazioni; e poi di migliore qualità dei dati, in quanto la correzione degli errori viene effettuata "alla fonte", e di riduzione delle attività connesse alla gestione delle dichiarazioni. Dal secondo punto di vista, i vantaggi per i contribuenti, chi si avvale di tale modalità di presentazione acquisisce la certezza di aver assolto agli obblighi verso l'Amministrazione; sulla base dell'attestato dell'avvenuta ricezione della dichiarazione; inoltre, aumenta la possibilità di ovviare alle eventuali irregolarità entro il termine di presentazione della dichiarazione successiva, a causa della disponibilità in tempi brevi delle dichiarazioni eseguite in via telematica.

Con riferimento alle modalità pratiche con cui avviene la presentazione delle dichiarazioni, i dati che pervengono in via telematica sono "protetti" e viaggiano attraverso la rete in modo tale da poter essere letti esclusivamente da chi ha compilato la dichiarazione telematica e dall'Amministrazione cui la dichiarazione viene presentata. L'adozione di particolari tecniche di "autenticazione" dei dati, nella specie della firma digitale, permette infine di individuare con certezza da chi provengono e, quindi, di contestare le eventuali irregolarità commesse all'effettivo responsabile. Tali interessanti e proficue utilità, insieme all'evoluzione delle tecnologie Internet e all'imminente approvazione delle regole nazionali in materia di sottoscrizione digitale, consentiranno poi in tempi brevi di

estendere questa modalità di presentazione anche a coloro che compilano autonomamente la dichiarazione dei redditi, senza l'assistenza di alcun intermediario: evitando così ai contribuenti, che utilizzeranno questa opportunità, l'onere di compilazione e presentazione del modello cartaceo.

Dal punto di vista tecnico-esecutivo, presupponendo anche in questo caso che i soggetti abilitati alla nuova modalità siano già dotati di una postazione informatica adeguata (non sono richieste grandi capacità), il software necessario per lo svolgimento del servizio e le relative istruzioni vengono distribuiti gratuitamente dall'Amministrazione finanziaria; non è previsto poi alcun costo a carico degli intermediari neanche per la trasmissione dei dati e per l'accesso alle informazioni disponibili attraverso il sito web del servizio telematico, operazione che si farà mediante il collegamento ad un numero verde. Per svolgere l'intera attività, il Ministero consegna ai soggetti abilitati al servizio le istruzioni su *floppy-disk* e una busta chiusa che contiene: nome utente e password per la connessione in rete, che vanno utilizzate per configurare il proprio elaboratore elettronico, con le modalità espresse in apposite istruzioni; chiave e password di accesso al sito Web del servizio, che vanno utilizzate ogni qualvolta richiesto dalle applicazioni del servizio stesso; infine il c. d. "PINCODE", cioè il numero identificativo da utilizzare, seguendo le istruzioni, durante la generazione delle chiavi asimmetriche (chiave pubblica e chiave privata) che permettono il calcolo dei codici di autenticazione, che vengono trasmessi dall'utente, unitamente ai file cui si riferiscono.

A questo proposito, si deve rilevare come il servizio che si sta descrivendo rappresenti la prima vera applicazione del sistema di firma digitale introdotto nel nostro ordinamento dal DPR 513. Tenuto conto infatti che la presentazione della dichiarazione in via telematica sostituisce per i soggetti incaricati (art. 12, comma II, del DPR 600/73) il modello cartaceo, doveva necessariamente essere adottato un sistema che consentisse, da una parte, l'identificazione certa di chi presenta la dichiarazione; dall'altra il riconoscimento certo di una qualsiasi modifica successiva ai dati in essa contenuti. Si dovevano cioè assicurare modalità di svolgimento del servizio che consentissero di identificare in modo "certo e non contestabile" il "responsabile" della presentazione telematica, creando una corrispondenza univoca tra questi e il documento trasmesso, nonché con il suo contenuto, con l'obiettivo di garantire sia l'Amministrazione che il contribuente. Da queste esigenze la decisione di adottare i sistemi di crittografia asimmetrica, gli unici in grado, attualmente, di dare soddi-

sfare le garanzie richieste. Così, per ottenere il documento adeguatamente "protetto", ciascun utente e l'Amministrazione possiedono una coppia di chiavi asimmetriche, di cui una è "privata" e nota solo al titolare, mentre l'altra è "pubblica" ed è nota a entrambi⁷⁹. Come è stato disciplinato nell'ambito del DPR 513⁸⁰, a carico dell'utente è la custodia della chiave privata, che va mantenuta segreta e adeguatamente protetta da uso indebito: quindi affidare a terzi l'utilizzo della chiave privata non modifica le proprie responsabilità personali nei confronti dell'Amministrazione. Viene anche previsto l'uso della funzione di *hash*⁸¹ sui documenti contenenti le dichiarazioni⁸².

⁷⁹ Come si legge nell'Appendice di "Unico 99-Persone Fisiche", Fascicolo 1, "Modello base per la dichiarazione e istruzioni", edito dal Ministero delle Finanze, p. 55: "Ogni parte autentica i suoi documenti usando la sua chiave privata e li invia al destinatario. Questo legge e controlla il codice di autenticazione utilizzando la chiave pubblica del mittente. Sulla base della documentazione consegnata dalla DRE e utilizzando il software distribuito dall'Amministrazione finanziaria, ciascun utente provvede a creare l'"Ambiente di sicurezza" che consiste nel: - generare la chiave pubblica e la chiave privata; - generare la richiesta di iscrizione nel registro degli utenti, che contiene, oltre alla chiave pubblica, gli elementi utili ad identificare il suo possessore; - trasmettere, utilizzando il servizio telematico, la richiesta di iscrizione. L'Amministrazione finanziaria, utilizzando il sistema di validazione, al momento della ricezione della richiesta e in modo completamente automatico: - verifica, tramite il PINCODE, la rispondenza dei dati contenuti nella richiesta di iscrizione con quanto constatato personalmente dall'ufficio finanziario al momento dell'abilitazione dell'utente al servizio telematico; - verifica che l'utente non risulti già iscritto nel registro e, in tal caso, che l'iscrizione risulti o meno valida.

In caso di esito positivo dei controlli, l'Amministrazione finanziaria, tramite il sistema di validazione, iscrive l'utente nell'apposito registro e restituisce un'attestazione in formato elettronico, munita del codice di autenticazione. L'esito negativo dei controlli, che comportano l'impossibilità di iscrivere l'utente nel registro, vengono comunicati tramite il servizio telematico".

⁸⁰ In base al combinato disposto del suo articolo 1, lett. e (relativo alla definizione di "chiave privata"), dell'art. 9 comma I (responsabilità degli utenti del sistema di firma digitale) e dall'art. 8 DPCM 8 febbraio 1999.

⁸¹ "Al contrario, è obbligatorio l'utilizzo del software che: - sottopone il file che contiene i dati delle dichiarazioni ad una funzione che calcola un riassunto del file stesso; - contrassegna il riassunto del file sfruttando algoritmi matematici che utilizzano la chiave privata, ottenendo in tal modo il codice di autenticazione, che viene trasmesso unitamente al file cui si riferisce. Lo stesso software che calcola il codice di autenticazione, provvede a contrassegnare i dati, utilizzando algoritmi matematici che utilizzano una chiave costruita dinamicamente, tale da garantire che i dati contenuti nel file possano essere letti solo dall'Amministrazione, in modo da garantire la riservatezza dei dati" (così dall'Appendice di "Unico 99-Persone Fisiche", Fascicolo 1, *cit.*).

⁸² Anche in questo caso aiutano le istruzioni impartite dalla stessa Amministrazione

Una volta pronto il documento, deve essere inviato al Ministero: questo avviene attraverso Internet ed una "Rete Privata Virtuale" che consente una trasmissione sicura delle informazioni riservate. Alla ricezione l'Amministrazione compie i necessari controlli, sia relativi alla trasmissione, sia per i contenuti delle dichiarazioni crittate, e quindi invia idonea ricevuta al commercialista che aveva attuato l'intera operazione per il proprio cliente.

Dalla prima applicazione di questo sistema, con riferimento alle nuove attività del commercialista ad esso connesse, è possibile realizzare quali potenzialità sarà possibile sviluppare in un futuro non più così remoto: i professionisti interessati sono oltre 100.000, mentre gli utenti chiaramente molti di più, ed entrambi potranno solo guadagnare da una migliore gestione delle informazioni da parte dell'Amministrazione finanziaria.

Nella prima applicazione del sistema descritto sono state inviate per via telematica oltre l'80% delle dichiarazioni dei redditi. Ciò ha conferito all'Italia il primato mondiale nel settore.

L'Ottimismo sembra dover prevalere.

finanziaria che, nello spiegare l'attività svolta al momento della ricezione della dichiarazione, mostrano come viene poi utilizzata in concreto la funzione di *hash*: "Il controllo del codice di autenticazione, in particolare, consiste in: - decodifica del codice di autenticazione, mediante la chiave pubblica dell'utente; se l'operazione va a buon fine, è certo che l'origine del file è proprio quella dichiarata al momento della trasmissione (autenticazione del mittente); - ricalcolo del riassunto del file; se il riassunto coincide con quello ottenuto effettuando l'operazione descritta al punto precedente, il file non è stato alterato successivamente al calcolo, da parte dell'utente, del codice di autenticazione (integrità del dato)". Anche in questo caso non si capisce bene però sulla base di quale documento viene effettuato il "ricalcolo". Se infatti applicando la chiave pubblica del mittente apro il codice di autenticazione, dovrei ottenere direttamente la sola impronta: e allora come faccio a ricalcolare il riassunto del file?

Paola Di Salvatore

I contratti informatici

SOMMARIO: 1. Origini del contratto informatico. - 2. Che cos'è il contratto informatico - 3. Quale disciplina applicabile ai contratti informatici? Riflessioni sui primi inquadramenti sistematici - 4. Analisi delle clausole vessatorie inserite nei contratti informatici alla luce dell'orientamento del legislatore europeo - 5. L'importanza dell'inserimento della clausola di buon funzionamento nella stipula di un contratto informatico - 6. Analisi morfologica dei contratti informatici. - 7. I contratti relativi all'hardware. - 7.1 Il contratto di vendita di hardware. - 7.2 Il contratto di leasing di hardware. - 8. I contratti relativi al software. - 8.1. Il contratto di compravendita di software. - 8.2. Il contratto di licenza di software. - 8.3. Il contratto di licenza d'uso di software. - 8.4. Il contratto di licenza a strappo (*shrink-wrap license*). - 8.5. Il contratto di *shareware* e di *freeware*. - 8.6. Il contratto di leasing di software. - 8.7. Il contratto di sviluppo di software. - 9. Lo studio di fattibilità e le specifiche funzionali nel contratto di sviluppo di software. - 10. Lo sviluppo del programma. - 11. Sulle verifiche in corso d'opera nel contratto di sviluppo di software. - 12. Il collaudo e l'accettazione nel contratto di sviluppo di software. - 13. La titolarità del diritto di autore nel contratto di sviluppo di software. - 14. I contratti di assistenza e di manutenzione del software. - 15. L'attività di manutenzione alla luce del D. Lgs. n. 518/92. - 16. I contratti per la fornitura di servizi informatici. - 16.1. I contratti di consulenza. - 16.2. Il contratto di *body rental*. - 16.3. Il contratto di *disaster recovery*. - 16.4. I contratti di *computer services contract*. - 17. I contratti di assistenza e di manutenzione.

1. Origini del contratto informatico

Il contratto informatico ha avuto la sua origine negli anni '60 in America.

All'epoca vigeva il sistema del *bundling*, caratterizzato dalla congiunta vendita da parte delle grandi imprese produttrici di hardware sia del macchinario, come bene principale, che degli accessori, a volte opzionali a