sui dati, opere o altri elementi inseriti in una banca dati... il segreto industriale..., la riservatezza... l'accesso ai documenti pubblici...».

Un'ultima considerazione al riguardo. Quando si tratti di banche-dati registrate nelle memorie di un computer, la loro tutela giuridica non va confusa non solo con quella accordata ai singoli documenti o elementi in essa contenuti, ma neppure con quella (di cui al D.Lgs. 518/92) al software realizzato per consentire all'utente informatico l'accesso e la selezione del materiale[235]. Infatti, se anche è vero che in tale fattispecie la «disposizione del materiale» in banca-dati (cioè uno degli elementi di originalità di esso) costituisce un fatto virtuale (non statico ma dinamico) dipendente in sostanza dal software, è pur vero che l'originalità del sistema teorico di ricerca e di selezione (cioè l'algoritmo) non può essere tenuta in considerazione quanto al riconoscimento di un diritto d'autore sul software, mentre può ben esserlo, invece, ai fini del riconoscimento di un diritto d'autore sulla banca-dati.

Inoltre è fin troppo evidente che i due diritti divergono sia quanto alla individuazione degli autori, sia quanto alla natura dell'attività svolta; altro è, infatti, saper scegliere il materiale da includere nella banca-dati e, come di solito avviene, classificarlo (o comunque sottoporlo ad un trattamento propedeutico a quello), altro è, invece, saper svolgere l'algoritmo in un complesso di istruzioni applicabili dal computer.

Da quanto sopra si deduce che il rapporto tra banca-dati e software di ricerca per essa adottato si caratterizza, da un lato, per la diversità dei diritti d'autore concernenti l'una o l'altro, ma, dall'altro lato, per l'intreccio che si crea tra l'una e l'altro, in quanto uno degli elementi costitutivi della nozione giuridica di banca-dati protetta dal diritto d'autore ai sensi del D.Lgs. 169/99 (e, cioè, l'originalità della disposizione del materiale consultabile e del sistema di accesso ad esso e di selezione del medesimo) può essere ravvisato proprio nel software di ricerca o, come oggi si usa dire, nel «*motore di ricerca*» creato per la sua consultazione.

[235] Dispone, infatti, l'art. 1 (comma 3) della Direttiva 96/9/CE: «La tutela della presente direttiva non si applica ai programmi per elaboratori utilizzati per la costituzione o il funzionamento di banche dati accessibili grazie a mezzi elettronici».

Capitolo VII

L'IMPATTO DELL'INFORMATICA SULLA PROVA DOCUMENTALE

Sommario: *Sezione I* - Il documento informatico: 205. Il Documento Informatico. – 206. Nozione tecnica. – 207. Il documento informatico secondo la dottrina. – 208. La nozione legislativa di documento informatico. – 209. Il documento informatico nella disciplina legislativa della firma digitale (D.P.R. 445/2000). – 210. La disciplina del documento informatico. – 211. La natura giuridica del documento informatico. – 212. Il valore giuridico del documento informatico. – 213. Firma elettronica, firma digitale e valore giuridico del documento elettronico. – 214. La firma digitale e la firma elettronica da un punto di vista tecnico. – 215. La firma digitale da un punto di vista strutturale: il Certificatore. – 216. Il valore giuridico del documento informatico nel sistema italiano di firma digitale o elettronica. – 217. Il notariato informatico. – 218. Le applicazioni della firma digitale ed il notaio. – 219. La disciplina normativa della firma digitale ed il notaio. *Sezione II* - Ulteriori informazioni sul tema del documento informatico e sulla firma elettronica: 220. Innovatività dirompente del documento informatico e della firma elettronica in tutto l'ordinamento giuridico e, in particolare, nel diritto civile. – 221. La registrazione dei BIT nelle memorie del computer: è «scrittura»? – 222. Il tramonto della firma autografa. – 223. I primi passi del legislatore verso il riconoscimento del documento informatico come documento scritto. – 224. La riproduzione informatica della firma autografa. – 225. La firma digitale: caratteristiche e funzione essenziali. Chiave privata e chiave pubblica: un sigillo, non una firma. – 226. Differenza delle chiavi asimmetriche rispetto a quelle simmetriche. – 227. La superiorità dei sistemi a chiavi asimmetriche. – 228. Firma digitale e firma elettronica avanzata: la ricomprensione della prima nella seconda. – 229. La firma elettronica avanzata nel quadro dell'automazione sostanziale. I vantaggi che la firma autografa non soddisfaceva. In particolare: la segretazione dei messaggi. – 230. La firma elettronica «debole». – 231. La funzione del certificatore (terzo fidefaciente) nel sistema della firma digitale. – 232. Il «dispositivo di sicurezza» per la generazione della firma digitale e la «smart-card» che lo contiene. – 233. La «firma qualificata» (o sicura che dir si voglia). – 234. Il carattere personale e indisponibile della smart-card e del dispositivo che contiene. – 235. La firma digitale autenticata. – 236. Il valore probatorio del documento informatico a seconda del tipo di «firma» di cui è munito. – 237. Querela di falso e responsabilità del querelante. – 238. La responsabilità eventuale del titolare della firma digitale in caso di accoglimento della querela di falso. – 239. Conclusioni.

Sezione I

Il documento informatico

205. *Il Documento Informatico.* – Nell'esporre le caratteristiche del computer, ed il suo impatto positivo nelle varie attività dell'uomo, si è anche sottolineata la sua importanza nell'attività di documentazione, sia con riferimento alla fase della redazione, sia con riferimento a quella della gestione (intesa come elaborazione, ricerca e comunicazione) del documento stesso. Infatti, fin dagli anni sessanta, le metodologie per la redazione di documenti sono state sempre più collegate all'introduzione e all'utilizzazione delle nuove tecnologie, ed in particolare dell'informatica: e sono apparsi, dunque, in misura sempre crescente, documenti prodotti da sistemi automatizzati basati su elaboratori elettronici e definiti, quindi, documenti informatici, o elettronici[236]. Ed anzi, è la natura stessa del computer, quella di macchina atta a gestire l'informazione in senso ampio, e quindi a reperire, trattare e comunicare i dati, nonché a conservarli in maniera organizzata nel tempo, a rendere i sistemi informatici gli strumenti più adatti, per efficienza ed economicità, all'attività di documentazione[237].

[236] Nel presente scritto i due termini vengono considerati come sinonimi, ma non è rara in dottrina una loro distinzione: si veda, a tale proposito, E. Giannantonio, *Manuale di diritto dell'informatica*, CEDAM, Padova 1997, pp. 365 e 367, e A. Martino (a cura di), *Nuovo regime giuridico del documento informatico*, Franco Angeli, Milano 1998, p. 23. Sulla differenza tra elettronica e informatica v. anche i §§ 2 e 3 del libro di R. Borruso e C. Tiberi citato in prefazione.

[237] «In un mondo abitato da poche centinaia di migliaia di esseri umani, che traevano il loro sostentamento dalla caccia e dalla pesca, poteva bastare l'uso dalla *parola orale* per comunicare col prossimo e tramandare ai posteri le esperienze di vita. Cresciuta la popolazione ad alcuni milioni grazie all'agricoltura, fu necessario, per organizzare la collettività e darle un minimo di consapevolezza, ricorrere alla *scrittura*. Quando poi, per effetto dei traffici sempre più intensi ed estesi e dello sviluppo materiale e morale conseguente, si sentì l'esigenza di partecipare le conquiste del pensiero ad un'umanità di quasi mezzo miliardo di persone, nacque la *stampa* e la vita fu dominata dall'uso dei documenti cartacei. Quando, infine, nel XX secolo l'umanità raggiunse il miliardo di persone, i mezzi di comunicazione si arricchirono – oltreché del telegrafo di ottocentesca memoria – del telefono, della radio, del cinema, della televisione. Oggi, alle soglie del XXI secolo, con una popolazione mondiale di circa sei miliardi, la storia, cominciata con l'invenzione della scrittura, ha raggiunto – quasi ad un appuntamento provvidenziale – la terza, decisiva tappa del suo sviluppo: l'uso massivo del computer, cioè di uno strumento finalmente adeguato alle odierne esigenze. Scrittura, stampa, computer devono essere, dunque, considerate in una visione di insieme, lungo una medesima direttrice di progresso, anche se il computer è ben più che un mezzo di memorizzazione e di comunicazione. E come la scrittura e la stampa hanno permeato tutti gli aspetti della nostra vita modificandoli radicalmente (a cominciare dal diritto: prima orale, poi scritto, infine stampato), egualmente è facile prevedere che avvenga per il computer e che, cioè, il suo uso diventi universale e rivoluzionario» (R. Borruso-C. Tiberi, *L'informatica per il giurista. Dal* bit *ad Internet*„ Giuffré, Milano 2001, p. XVII).

Dimostrazione di ciò è la progressiva sostituzione di sistemi gestionali automatizzati a quelli «manuali», applicati nelle forme tradizionali nelle stazioni operative degli uffici pubblici o privati, nonché la diffusione e l'importanza sempre maggiore dei documenti provenienti da un sistema di elaborazione elettronica: si ha, infatti, sempre più occasione di utilizzare certificati elettorali o di stato civile rilasciati da anagrafi computerizzate, documentazione elettronica proveniente dalle conservatorie immobiliari o dal catasto[238], scontrini emessi da casse automatiche, tabulati contenenti massime giurisprudenziali. E non bisogna dimenticare le numerose attività rese possibili dai servizi introdotti dalla rete telematica Internet, nuovo *medium* di informazione e comunicazione: recente esempio, la possibilità per il notaio di eseguire «on line» gli adempimenti in materia di trascrizione, di voltura e di registrazione degli atti di compravendita di immobili, utilizzando il modello unico informatico[239].

Alla base di tale processo, e risultato dello stesso, si pone il documento informatico, cioè il documento prodotto dall'elaboratore elettronico, di cui ora occorre analizzare la nozione e le caratteristiche.

206. *Nozione tecnica.* – Per meglio comprendere in che cosa consista esattamente il documento informatico è necessario, sia pure in maniera estremamente sintetica e semplificata (ed a costo di ripetere concetti già espressi nelle pagine precedenti, ma proprio al fine di introdurre la nuova «*res*» ed evidenziare modalità ed ambiti in cui verrà intesa l'espressione in questa parte dello scritto), prendere le mosse da alcuni principi base dell'informatica.

Il computer, sia in un momento dinamico, di elaborazione dei

[238] Così L. Grisostomi Travaglini, *Il trasferimento elettronico dei documenti*, Tesi di dottorato, Roma 1995; per quanto riguarda le conservatorie immobiliari automatizzate si veda R. Zagami, *L'automazione delle conservatorie immobiliari*, in *Informatica e Diritto*, 1995, 2, pp. 97 e ss.

[239] Il modello unico informatico è quella particolare procedura che permette ai notai di adempiere per via telematica gli obblighi inerenti la registrazione, trascrizione e voltura degli atti relativi a diritti sugli immobili (ed altri atti tra vivi e *mortis causa*). Su tale innovazione si veda oltre, il paragrafo 221.

dati o di trasmissione degli stessi, sia in un momento statico, di archiviazione e conservazione dei dati elaborati, lavora con realtà elettroniche digitali (cioè basate su un sistema binario di interpretazione della realtà, corrispondente ad una sequenza di combinazioni di 0 e di 1): a livello circuitale o di reti telematiche nel primo caso, in supporti magnetici o ottici corrispondenti alle memorie ausiliarie nel secondo.

Il singolo circuito, o la singola parte di materiale magnetico o ottico, che può avere un duplice valore («passa corrente» oppure «non passa corrente», per il circuito interno all'unità centrale, «magnetizzato» oppure «non magnetizzato», per la superficie della memoria ausiliaria magnetica, «buco» o «piano», per quella della memoria ausiliaria ottica, il CD-ROM) prende il nome di *bit*[240]. Un insieme di *bit*, a cui è possibile attribuire un significato (ad esempio una lettera dell'alfabeto per gli scritti, oppure una nota musicale per i suoni, o ancora una determinata tonalità di colore per le immagini), prende il nome di *byte*, che viene inoltre considerato l'unità di misura per le varie componenti del sistema di elaborazione dati.

Grazie all'evoluzione repentina ed esponenziale delle tecnologie informatiche, oggi è possibile, in base a strumenti di acquisizione delle informazioni particolarmente avanzati, rendere una qualsiasi realtà percepibile dai nostri sensi in maniera gestibile dal computer[241], in particolare quindi attraverso *byte*, cioè in formato digitale[242]. Anzi, è proprio il concetto di informazione, a causa dell'interazione con i nuovi strumenti automatici di gestione della stessa, a cambiare, a diventare informazione automatica, informatica.

Così, alla luce di tale processo e di queste modalità operative, informazione è sicuramente un testo scritto, ma è anche un suono,

[240] Il termine *bit* deriva dalla crasi di «*binary digit*» (cifra binaria) ed è utilizzato per individuare l'unità minima di informazione che l'elaboratore è in grado di ricevere.

[241] E riferirsi a tutti e cinque i sensi non è più esagerazione fantascientifica: infatti si possono segnalare diverse sperimentazioni sia per simulare la percezione olfattiva che quella del gusto.

[242] Si vedano a tale proposito interessanti teorie proposte (nonostante lo stile letterario che lascia un po' a desiderare) da Nicholas Negroponte, direttore del M.I.T. (Massachussets Institute of Tecnology) di Boston, che in un suo libro sostituisce il bit all'atomo in una peculiare interpretazione della realtà (così N. Negroponte, *Essere digitali*, Sperling&Kupfer, Milano 1995).

un odore, un'immagine: tutti elaborabili attraverso un sistema automatizzato.

Se il computer permette di ampliare a questo livello il concetto di informazione, allora anche il concetto di documento ne risulta altrettanto ampliato.

Le informazioni, infatti, vengono conservate all'interno delle memorie del computer (momento statico), o elaborate nel microprocessore (momento dinamico), raggruppate a seconda delle loro caratteristiche comuni: insieme di istruzioni che devono essere eseguite dall'elaboratore per svolgere una determinata funzione, nel caso di informazioni che costituiscano un software; gruppo di pagine che formano un determinato testo leggibile; insieme di colori che compongono un'immagine, o insieme di immagini che realizzano un'immagine in movimento, un filmato; infine, insieme di suoni che costituiscono, ad esempio, un brano musicale. Il termine inglese usato per individuare questi gruppi di informazioni è «*file*» o «*record*», che può essere tradotto in italiano con «cartella» o «documento»[243].

Pertanto, tenendo presente le modalità di gestione delle informazioni da parte del computer, per documento[244] oggi può essere inteso un testo, ma anche un'immagine, oppure un insieme di imma-

[243] Un *file* riunisce quindi un insieme di *byte*, di dati che collegati tra loro vanno a costituire un insieme di informazioni, che hanno in comune la caratteristica di rappresentare specifiche realtà, anche di natura diversa: come, ad esempio, le istruzioni che compongono un determinato software, cioè un determinato programma per computer (e avranno allora, nel linguaggio informatico MS-DOS, un nome con estensione «.exe»); o le pagine di un documento (e potrà avere un nome con estensione «.doc» oppure «.txt»); o ancora quella di identificare i *pixel* che compongono un'immagine (il cui nome sarà quindi caratterizzato dall'estensione «.jpg» o «.bmp»), o i suoni che contribuiscono a costituire un brano audio (e il loro nome potrà avere come estensione «.wav»).

[244] Che, tradizionalmente, viene inteso come «qualsiasi oggetto, qualsiasi cosa idonea a far conoscere un fatto, diversa dal testimone, che è una persona che narra, e non una cosa che rappresenta (F. Carnelutti, *Documento - Teoria moderna*, in *Nov. Dig. It.*, VI, Torino 1957, p. 85 ss.). Ma relativamente alla nozione di «documento», mancando nel nostro ordinamento una definizione di carattere generale, si veda anche altra dottrina che considera documento in largo senso «ogni rappresentazione materiale destinata ed idonea a riprodurre una data manifestazione del pensiero (...)», per poi sottolineare che «come il mezzo comune di rappresentazione materiale del pensiero è lo scritto, così i documenti di gran lunga più importanti sono le scritture» (così G. Chiovenda, *Principi di Dir. Proc. Civile*, 3ª ed., Napoli 1923, p. 842).

gini, o ancora un suono o un insieme di suoni, oppure tutte queste realtà (testo, immagini e suoni) insieme[245].

Considerando quindi tali nuove possibilità, meglio si intende la nozione di documento elettronico, come documento, inteso nel senso ampio ricordato, prodotto da un sistema informatico[246]. Ma vediamo ora come è stato concepito tale documento secondo la dottrina più attenta alle nuove tecnologie.

207. *Il documento informatico secondo la dottrina.* – Seguendo la dottrina prevalente[247], è possibile distinguere diversi tipi di documenti informatici. La classificazione più opportuna degli stessi, infatti, può essere fatta in base a tre momenti del processo elaborativo e, precisamente, in base all'*input*, all'*output* e al modo di elaborazione. In particolare, con riferimento al primo dei tre, cioè quello dell'immissione nelle memorie dell'elaboratore, si possono individuare i documenti informatici originari e i documenti informatici derivati: questo a seconda che l'acquisizione del documento avvenga attraverso la riproduzione meccanica di un fatto esterno, e in particolare di un precedente documento scritto, oppure ad opera dell'uomo attraverso apposite macchine memorizzatici (dalla tastiera al riconoscitore di voce).

In base al *modo di elaborazione*, invece, può essere opportuno distinguere i casi in cui la riproduzione è diretta ad ottenere un documento identico per forma e contenuto al documento originario, dai casi in cui la riproduzione consiste nella trascrizione del contenuto del documento in un linguaggio elettronico. Nella prima ipotesi sarebbe compresa, ad esempio, l'acquisizione di documenti attraverso apparecchiature *scanner*, mentre nella seconda l'applicazione di metodologie *O.C.R.* agli scritti acquisiti in tal modo (diverso è il risultato finale: un'immagine tendenzialmente non accessibile nel primo caso, realtà che ha comunque sempre interessato il legislatore nei suoi interventi volti a conferire al documento elettronico un valore giuridico – è il caso delle varie norme che parlano di «supporti di immagine», come ad esempio l'art. 2220 c.c., che danno particolare affidabilità proprio per la loro immodificabilità –, un testo accessibile e modificabile nel secondo).

I documenti informatici, infine, si differenziano in base all'*output*, ossia al modo in cui vengono emessi dall'elaboratore. Al riguardo sono stati distinti in due classi: i documenti elettronici *in senso stretto* e i documenti elettronici *in senso ampio*.

I primi sono conservati in forma digitale nella memoria centrale, ovvero nelle memorie di massa dell'elaboratore, e non possono essere letti, o comunque percepiti dall'uomo, se non attraverso l'uso dello stesso elaboratore che renda acquisibili e comprensibili i segnali digitali dai quali sono costituiti: ad esempio, mostrando a video il testo o l'immagine, oppure facendo ascoltare il brano musicale. Chiaramente i documenti così formati avranno un diverso grado di durata nel tempo, secondo le caratteristiche del supporto usato. Tale durata varia, quindi, dal caso in cui i documenti siano contenuti nelle memorie circuitali RAM (*Random Access Memory*), che sono di carattere volatile, ossia si cancellano automaticamente appena viene spento l'elaboratore; al caso in cui siano contenuti in nastri o in dischi magnetici, che rimangono memorizzati finché un intervento umano non provveda a cancellarli o modificarli; fino al caso estremo in cui vengano destinati a perdurare in forma inalterabile nel tempo, ossia contenuti in memorie ROM (*Read Only Memory*), o memorizzati su supporti ottici.

I documenti informatici *in senso ampio* sono, invece, tutti quei documenti formati dall'elaboratore mediante i propri organi di *output*[248]. Tali documenti non sono necessariamente testuali e in forma digitale, ma possono essere costituiti da un testo alfanumerico, un di-

[245] Nel qual caso si avrà un documento multimediale (sui prodotti multimediali, e sulla loro tutela, si veda M.G. Losano, *Scritto con la luce. Il disco compatto e la nuova editoria elettronica*, Ed. Unicopli, Milano 1988, pp. 1-128, G. Ciacci, *Multimedialità e CD-ROM: profili giuridici*, in *Economia e Diritto*, Franco Angeli, 1993, pp. 989-1011.

[246] Relativamente al concetto di «sistema informatico» si veda il precedente paragrafo 149.

[247] In particolare, E. Giannantonio, *Manuale di diritto dell'informatica*, cit., p. 366, ma anche, dello stesso autore, *Il valore giuridico del documento elettronico*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, Vallardi, 1986, p. 261; si può poi fare riferimento a R. Borruso, *Computer e diritto*, vol. II. *Problemi giuridici dell'informatica*, Giuffrè, Milano 1988, p. 216 e ss., e, con particolare attenzione al valore giuridico del documento prodotto attraverso un sistema informatico, di cui si parlerà oltre, L. Montesano, *Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Il diritto dell'informazione e dell'informatica*, 1987, p. 25, e nella voce *Documento giuridico* dell'Enciclopedia giuridica.

[248] Come si è già detto, sono organi di *output* tutti gli apparati hardware del sistema informatico adibiti a mostrare il risultato dell'elaborazione dei dati: ne costituisce esempio il monitor del computer, la stampante, e in genere ogni dispositivo meccanico comandabile elettronicamente (come ad esempio il timone di un missile).

segno, un grafico o un'immagine fotografica, e possono essere resi su un supporto cartaceo, una scheda o un nastro perforato, un microfilm o, comunque, un qualsiasi oggetto materiale formato da una macchina collegata con un elaboratore.

In sostanza, dunque, i documenti informatici *in senso stretto* sono destinati ad essere utilizzati esclusivamente attraverso l'elaboratore; i documenti informatici *in senso ampio* sono formati dall'elaboratore per essere letti o comunque percepiti dall'uomo senza l'intervento dello stesso computer. Esempi più comuni di documenti elettronici in senso ampio sono i tabulati prodotti dalle stampanti e i grafici e i disegni realizzati dai plotter; esempi di documenti elettronici in senso stretto sono, invece, le memorie circuitali dell'elaboratore, ovvero le memorie magnetiche, come i nastri o i dischi, o, ancora, le più recenti memorie ottiche, intese non tanto come supporto fisico, ma come i file o i record in essi contenuti.

Al di là comunque delle definizioni e delle distinzioni di matrice teorica, occorre ora esaminare come il documento prodotto attraverso l'elaboratore elettronico venga concepito a livello del diritto positivo, tenendo comunque in una particolare attenzione i rilievi tecnico-informatici in precedenza riportati.

208. *La nozione legislativa di documento informatico.* – Una prima nozione di «documento informatico» è stata introdotta nel nostro ordinamento dall'art. 3 della legge 23 dicembre 1993 n. 547, in materia di criminalità informatica[249], con la quale il legislatore ha inserito l'art. 491-*bis* nel codice penale, all'interno del capo III del titolo VII in materia di falsità in atti[250]. Tale articolo, nel suo secondo comma[251], testualmente riporta che «*per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*».

[249] Per un commento a questa legge si veda R. Borruso-G. Buonomo-G. Corasaniti-G. D'Aietti, *Profili penali dell'informatica*, Giuffré, Milano 1994, pp. XVIII-199, P. Galdieri, *Teoria e pratica nell'interpretazione del reato informatico*, Giuffré, Milano 1997, pp. XII-265; C. Sarzana, *Informatica e diritto penale*, Giuffré, Milano 1994.

[250] L'art. 491-*bis* non fa altro che riaffermare la nozione tradizionale di documento come entità materiale, solo «attualizzata» rispetto alla nuova realtà informatica (così P. Galdieri, *op. cit.*, p. 110).

[251] Nel primo comma la norma in esame, intitolata proprio «Documenti informatici», sancisce che «*se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*».

Un'attenta lettura della disposizione in commento[252], permette di rilevare che gli elementi su cui è stata posta l'attenzione del legislatore nel dettare tale definizione risultano essere due[253].

Innanzitutto, ha tenuto in considerazione il «supporto», e su di esso ha basato la sua definizione, riferendosi quindi essenzialmente al momento «statico» dell'attività di elaborazione elettronica; con ciò chiarendo una volta per tutte come i documenti provenienti da un sistema informatico costituiscano dei documenti giuridici[256], e ponendosi in tal modo in linea con la dottrina che individua il documento in una cosa corporale assolutamente distinta dal contenuto immateriale dello stesso (rappresentato nel caso di specie dai «dati o informazioni»)[255]. Ma cosa deve intendersi per «supporto informatico»?

Il legislatore, utilizzando tale espressione, sembrerebbe aver inteso riferirsi ad ogni memoria leggibile da parte di un computer, in cui i segnali oggetto di elaborazione abbiano natura digitale essendo

[252] Ma nello stesso senso si pone anche l'articolo 7 della legge, che nel modificare l'art. 621 del codice penale ai fini della configurabilità di alcune fattispecie di reato riguardanti la rivelazione del contenuto di documenti segreti, definisce documento «anche qualunque supporto informatico contenente dati, informazioni o programmi».

[253] Così L. Grisostomi Travaglini, *Il trasferimento elettronico dei documenti*, cit., p. 84.

[254] La obiezione che veniva sollevata alla tesi che faceva rientrare il documento informatico tra i documenti giuridici si fondava sulla mancanza nello stesso di una rappresentazione materiale, essendo i *bit* entità magnetiche non percepibili ai sensi umani. Per una convincente risposta a tale obiezione si veda E. Giannantonio, *Il valore giuridico del documento elettronico*, in *Riv. dir. comm.*, 1986, p. 276.

[255] Nel documento è possibile individuare di regola un elemento materiale ed un contenuto immateriale: l'elemento materiale risulta dall'attività di un soggetto che ha modificato con un mezzo idoneo la materia, in modo tale da consentire la rappresentazione di un fatto a chi la esamini (a tale proposito la dottrina tradizionale – si veda ad esempio F. Messineo, *Manuale di diritto civile e commerciale*, *Dottrine generali*, 8ª ed., Giuffrè, Milano 1952, p. 487 – distingue tra materia e mezzo); quanto al contenuto immateriale, qualunque fatto può essere documentalmente rappresentato. Così, secondo F. Carnelutti (*Documento - Teoria moderna*, cit., p. 86), si deve distinguere tra documenti dichiarativi e documenti narrativi, a seconda che essi contengano manifestazioni di pensiero o di volontà destinate a produrre effetti giuridici, oppure si limitino soltanto alla esposizione di un accadimento (nell'ambito dei documenti dichiarativi si differenzia poi tra documenti testimoniali e dispositivi, a seconda che la dichiarazione rappresentata sia di scienza o di volontà).

costituiti da «*bit*»: segnali magnetici, elettronici o ottici, la cui caratteristica peculiare è quella di costituire al tempo stesso una forma di scrittura da un lato, e cose materiali mobili distinte dal supporto che le contiene dall'altro. Si è quindi fatto riferimento, sia alle memorie magnetiche e ottiche, e quindi alle memorie ausiliarie (nelle quali il *bit* viene registrato mediante magnetizzazioni o smagnetizzazioni di determinati elementi del supporto, o attraverso la creazione o meno nella superficie di buchi con l'ausilio di un raggio laser), sia alle memorie elettroniche, e quindi a quelle circuitali interne all'unità centrale dell'elaboratore (nelle quali la registrazione dei *bit* avviene mediante il passaggio o la interdizione del flusso degli elettroni attraverso appositi apparati come valvole termoioniche, *transistor*, o microprocessori).

Il secondo elemento su cui si è concentrato il legislatore, nella redazione della definizione di documento informatico contenuta nell'art. 491-*bis*, riguarda quanto viene contenuto dal supporto.

Per aversi un documento informatico, secondo il citato articolo, è necessario che il supporto contenga dei dati o delle informazioni «aventi efficacia probatoria», ovvero «programmi specificamente destinati ad elaborarli». Ciò risulta come inevitabile conseguenza della *ratio* delle disposizioni normative in tema di falso documentale, che si muove e si esaurisce sul terreno delle prove.

In particolare, in ordine al primo inciso («dati o informazioni aventi efficacia probatoria»), si pone il problema di chiarire a quale efficacia probatoria il legislatore abbia fatto riferimento: se cioè egli abbia rinviato alle disposizioni normative che attribuiscono un'efficacia probatoria *a taluni* documenti informatici, o se invece abbia voluto attribuire *a qualunque* documento informatico l'efficacia probatoria tipica dei documenti tradizionali muniti di sottoscrizione autografa. Concordemente a quanto ritenuto dalla prevalente dottrina[256], deve ritenersi che la nozione di documento informatico è in parte una norma «in bianco», avendo voluto il legislatore tutelare penalmente esclusivamente quei documenti ai quali, in forza di altre disposizioni normative, debba essere riconosciuta efficacia probatoria. Con riferimento poi al secondo inciso («programmi specificamente destinati ad elaborare i dati e le informazioni contenute nel supporto informatico»), deve chiarirsi come il legislatore abbia sentito l'esigenza

[256] R. Borruso, *La tutela del documento e dei dati*, in Aa.Vv., *Profili penali dell'informatica*, cit., pp. 1-29.

di tutelare anche il programma poiché esso, consentendo l'elaborazione dei dati e delle informazioni, è inscindibilmente connesso al contenuto rappresentativo del documento informatico. Infatti, risulta facilmente comprensibile come anche un'alterazione del programma possa produrre quelle situazioni di danno o di pericolo alla pubblica fede che la sanzione penale mira a prevenire[257].

209. *Il documento informatico nella disciplina legislativa della firma digitale (D.P.R. 445/2000 e successive modifiche).* – Per completare l'indagine relativa alla nozione di documento informatico, anche in base alla disciplina normativa dell'argomento, occorre procedere all'esame di quanto recentemente disposto dal legislatore in materia di firma digitale[258], ma solo con riferimento all'argomento in esame: nei prossimi paragrafi si analizzerà quindi tale realtà in maniera particolareggiata.

Come si vedrà oltre, il sistema di firma digitale introdotto nel nostro Paese può essere considerato una fattispecie a formazione progressiva, che ha inizio dall'art. 15 comma 2 della l. 15 marzo 1997 n. 59, in materia tra l'altro di riforma della P.A. e di semplificazione amministrativa, che ha testualmente disposto: «*Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*».

In attuazione di quanto disposto da tale norma, nel novembre del 1997 il legislatore ha emanato il secondo atto della fattispecie a formazione progressiva[259], il D.P.R. 20 novembre 1997, n. 513, «Re-

[257] Così ancora L. Grisostomi Travaglini, *op. cit.*, p. 35.

[258] Cioè relativamente al sistema tecnico di validazione giuridica della documentazione elettronica scelto nel nostro Paese, quello appunto della firma digitale e di quella (in seguito alle recenti innovazioni, di cui si parlerà oltre nel testo) elettronica.

[259] Come si vedrà oltre nel testo, il terzo atto è consistito nell'emanazione delle norme tecniche in attuazione dell'art. 3 del D.P.R. 513, avvenuta con D.P.C.M. 8 febbraio 1999; altre fonti possono poi essere considerate il D.P.R. 28 dicembre 2000 n. 445, il T.U. sulla documentazione amministrativa (la cui portata innovativa è però relativa, avendo semplicemente abrogato e recepito quasi integralmente il D.P.R. 513/1997), il D.Lgs. 23 gennaio 2002 n. 10, che recepisce, questa volta modificando sostanzialmente l'intero sistema (con ambiti e modalità che si esamineranno in seguito), la Direttiva europea 1999/93/CE in materia di firme elettroniche, e infine il D.P.R. 7 aprile 2003 n. 137, ultimo atto legislativo che costituisce il regolamento recente disposizioni di coordinamento tra le precedenti norme in materia di firme elet-

golamento 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».

All'art. 1, lettera *a*), del D.P.R. 513/1997, ripreso integralmente dall'art. 1, lett. *b*) del D.P.R. 445/2000 che oggi disciplina la materia, viene indicata la nozione di documento informatico inteso come «*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*»[260]. Definizione che si allontana concettualmente da quella dettata dalla legge n. 547 del 1993: non viene, infatti, più preso in considerazione il supporto, ma, allo scopo di mantenere un livello più generico possibile, e comunque molto opportunamente, il modo di formazione. E questo non solo nella nozione indicata all'art. 1, lett. *b*), del D.P.R. 445, ma anche in quella all'art. 15, comma 2, della legge 59: nel primo caso in maniera meno evidente, aggiungendo la matrice «informatica» alla nozione della teoretica tradizionale di documento come «*res*» rappresentativa, analizzata in precedenza; nel secondo caso più direttamente, spostando l'attenzione dal documento in sé allo strumento utilizzato per la sua formazione[261].

Combinando il disposto delle due norme, il documento informatico può essere considerato una cosa rappresentativa ottenuta con l'ausilio di un sistema informatico. Non solo testi scritti quindi, ma anche suoni e immagini, fisse o in movimento: interpretazione che pone maggiormente in sintonia il costrutto normativo indicato con la realtà tecnica[262]. Costrutto che sembrerebbe porsi tra l'altro so-

troniche (come si vedrà oltre nel testo, regolamento previsto espressamente dall'art. 13 del D.Lgs. 10/2002).

[260] Stessa definizione si può trovare nel D.P.C.M. 22 ottobre 1999, n. 437, il regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, altra rivoluzionaria innovazione in avanzate fase di realizzazione.

[261] L'art. 15, comma 2, della legge 59 lascia intendere che«informatico non è tanto il documento o la rappresentazione in esso contenuta, ma lo strumento che serve a confezionare il documento, cioè, nei suoi multiformi modi di essere, l'elaboratore elettronico» (così F. De Santis, *Tipologia e diffusione del documento informatico. Pregresse difficoltà di un suo inquadramento normativo*, in *Il corriere giuridico*, 4, 1998, p. 387).

[262] Realtà già analizzata al paragrafo precedente, con riferimento al quale deve in questa sede ricordarsi, come si è detto nel testo, che «documento informatico» non è soltanto la versione digitale di un testo scritto cartaceo, ma anche suoni, immagini e immagini in movimento rese in *byte*.

stanzialmente in linea da una parte con la definizione di cui all'art. 491-*bis* c.p. (ed alla quale si rinvia, anche in relazione ai caratteri propri del documento informatico), dall'altra con le definizioni di documento proposte in dottrina, che pongono l'accento sulla capacità rappresentativa del documento, e cioè sulla sua idoneità a rappresentare un fatto esterno alla *res* documentale[263].

Così, costruita una definizione di documento informatico che considera sia le peculiari caratteristiche tecniche della nuova realtà, sia le considerazioni degli studiosi della materia, sia il dettato normativo che disciplina la materia, occorre ora riportare l'attenzione sulle distinzioni e classificazioni elaborate dalla dottrina e riportate in precedenza: e rilevare così che la grande varietà di documenti informatici solleva numerosi e diversi problemi giuridici. I documenti che costituiscono la riproduzione di fatti esterni o di altri documenti danno luogo al problema della loro conformità con il fatto o con il documento riprodotto; i documenti in senso stretto al problema, invece,

[263] Si faccia riferimento, in particolare, a F. Carnelutti, *Documento - teoria moderna*, in *Nov. Dig. it.*, VI, Torino 1957, 85 ss., ed a P. Guidi, *Teoria giuridica del documento*, Milano 1950, p. 46. Risulta interessante a questo punto riportare alcune definizioni legislative di documento informatico che si discostano, seppur di poco, da quelle analizzate nel testo: così in particolare nella Deliberazione A.I.P.A. n. 42/2001 («Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali»), ed il D.P.R. 13 febbraio 2001 n. 123, che introduce il processo telematico nel nostro ordinamento: l'art. 1 della prima fonte riporta le seguenti definizioni: a) *documento*: rappresentazione in formato analogico o digitale di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica; b) *documento analogico*: documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia; c) *documento analogico originale*: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi; d) *documento digitale*: testi, immagini, dati strutturati, disegni, programmi, filmati formati tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica, di cui sia identificabile l'origine e) *documento informatico*: documento digitale sottoscritto con firma digitale ai sensi dell'articolo 8 del Testo unico approvato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e del decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 e successive modificazioni. Invece nel D.P.R. 123/2001 si definisce il documento informatico come «la rappresentazione informatica del *contenuto* di atti, fatti o dati giuridicamente rilevanti».

della loro configurabilità come documenti scritti e, in particolare, come atti pubblici o scritture private o scritture contabili. Si tratta di problemi diversi che a volte si sovrappongono, ma che sarebbe grave errore non considerare in modo distinto[264]. Problemi che sono riconducibili, comunque, all'individuazione della natura giuridica del documento elettronico, ed alla determinazione del suo valore probatorio, come si vedrà nel prossimo paragrafo.

210. *La disciplina del documento informatico.* – Un fenomeno sociale così vasto e importante come quello del documento elettronico richiedeva certamente una regolamentazione giuridica: e, se in passato è stato possibile risolvere problematiche specifiche in base ad interpretazioni giurisprudenziali o dottrinarie (si pensi al problema del valore giuridico dei documenti trasmessi attraverso apparecchiature *telefax*), ciò non toglie che forte si sentisse l'esigenza di una soluzione legislativa non frammentaria e improvvisata, bensì coordinata e organica. Difatti in alcuni Paesi vennero emanate apposite norme per disciplinare i nuovi mezzi di documentazione[265].

In Italia, invece, fino alla recente produzione in materia di firma digitale, mancava una specifica disciplina; e le norme del codice civile che regolano i mezzi di prova in generale non prevedono, per evidenti ragioni cronologiche, i documenti informatici. Di conseguenza la giurisprudenza e la dottrina, di fronte alla nuova realtà, prive della guida del legislatore, hanno reagito negli anni in maniera diversa. La giurisprudenza penale ha ammesso, senza eccessivi contrasti, i nuovi mezzi di prova in base al principio del libero convincimento del giudice; la giurisprudenza e la dottrina civili, invece, sono state molto più esitanti e, in generale, contrarie alla possibilità di attribuire al documento elettronico il valore privilegiato di alcune prove tipiche e, in particolare, della scrittura privata o dell'atto pubblico.

[264] Ciò spiega perché non sia possibile assimilare tutti i documenti informatici ad uno solo dei tipi di prova previsti dal codice civile; come in alcuni casi i documenti informatici possano essere considerati riproduzioni meccaniche e in altri casi documenti scritti; come in altri casi ancora non possano essere equiparati a nessuna delle prove previste dal codice. In tali casi, peraltro, non deve essere esclusa ogni rilevanza giuridica del documento informatico, ma è necessario riconoscergli quella efficacia residuale che nel nostro, come il altri ordinamenti, è riconosciuto alle prove atipiche (così E. GIANNANTONIO, *Manuale di diritto dell'informatica*, cit., p. 368).

[265] Ad esempio in Argentina nel 1986 si riformò il codice civile con l'introduzione di un'apposita sezione dedicata proprio al valore giuridico del documento informatico.

Per quanto riguarda la dottrina, i primi studi sulla rilevanza giuridica dei documenti informatici in materia civile, apparsi nella seconda metà degli anni '80, riguardavano la possibilità o meno dell'applicazione analogica delle norme previste per gli altri mezzi di prova e, in particolare, delle norme in tema di riproduzioni meccaniche[266]. Da altri autori, invece, venivano poste in evidenza le analogie tra i documenti informatici e i documenti scritti: analogie evidenti nel caso dei tabulati, ma sussistenti anche nel caso di documenti memorizzati su dischi o nastri magnetici o su altri tipi di supporto[267].

Secondo un'autorevole opinione[268], le ragioni di questi contrasti e delle maggiori difficoltà in materia, derivavano dal fatto che si tendeva a considerare i documenti elettronici come una categoria unitaria; mentre occorreva, invece, porre in evidenza la grande varietà di documenti informatici e le differenze ben rilevanti che intercorrono tra loro.

Risulta a questo punto interessante, seppure sinteticamente, riportare le teorie che la dottrina aveva elaborato (in assenza di un dato legislativo certo, ed in presenza invece di un uso dei nuovi strumenti sempre più comune) relativamente alla *natura* ed al *valore* giuridico del documento elettronico.

211. *La natura giuridica del documento informatico.* – Il fondamentale quesito relativo al documento elettronico a cui si tentò di rispondere è se tale tipo di «*res*» prodotta mediante l'utilizzo di un sistema informatico potesse essere considerata o meno documento scritto. Oppure se, anche o alternativamente, dovesse essere assimilata ad altri tipi di rappresentazione, come ad esempio le riproduzioni meccaniche o fotografiche, previste dall'art. 2712 del codice civile, e le copie fotografiche di scritture, ex art. 2719 c.c.

Nel corso degli anni diversi autori si cimentarono nel rispondere

[266] La più autorevole formulazione di tale tesi è stata fatta da L. MONTESANO, *Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Il diritto dell'informazione e dell'informatica*, 1987, p. 25, e nella voce *Documento giuridico* dell'Enciclopedia giuridica.

[267] Un'interessante analisi della scrittura elettronica è contenuta nell'opera di R. BORRUSO, *Computer e diritto*, II. *Problemi giuridici dell'informatica*, Giuffrè, Milano 1988, p. 216 e ss., su cui si veda nel prossimo paragrafo.

[268] Così E. GIANNANTONIO, *Manuale di diritto dell'informatica*, cit., p. 366.

al primo problema, ed in genere in senso affermativo, attraverso differenti percorsi.

Così, particolarmente originale apparve la teoria che considerava il flusso degli elettroni come il nuovo inchiostro di cui l'uomo si serve, e le memorie elettroniche «la nuova carta, cioè il nuovo supporto su cui l'uomo scrive con il nuovo inchiostro»; i *bit* avrebbero costituito poi il nuovo alfabeto che l'uomo può utilizzare per esprimere qualsiasi opera del pensiero. Il documento elettronico veniva quindi considerato scrittura, intendendo per «scrittura» un insieme di segni riportati con qualsiasi mezzo e tecnica su un qualsiasi supporto, purché tali segni potessero essere letti e riletti anche a distanza di tempo[269].

Altra parte della dottrina[270] giungeva alle stesse conclusioni ma attraverso un percorso diverso, sulla base del rilievo che «la nozione di scrittura è più ampia di quello che è il suo normale modo di estrinsecazione e finisce per comprendere qualunque dichiarazione incorporata in un supporto materiale destinato a durare nel tempo». Il primo requisito di un documento scritto, secondo tale dottrina, è allora la *dichiarazione*, cioè l'atto con il quale si estrinseca il proprio pensiero con lo scopo di farlo conoscere ad una o più persone determinate, attraverso una combinazione di segni convenzionalmente stabiliti: non può, però, essere considerato documento scritto un semplice segno come, ad esempio, un'orma lasciata sul terreno, perché il suo autore nel momento in cui la pone in essere non esprime con essa alcun pensiero, né alcuna dichiarazione. Il secondo requisito che un documento scritto deve avere per essere considerato tale è la *incorporazione* in una realtà materiale. Un importante aspetto del documento, infatti, deriva dalla considerazione che il mezzo di redazione e la base di essa devono presentarsi stabilmente congiunti; *la dichiarazione*, in altre parole, *deve essere incorporata*. Necessario e sufficiente al concetto di scritto, pertanto, è che si lasci una traccia duratura e, quindi, leggibile sia al momento stesso in cui si scrive, così come a distanza di tempo. Il tipo di alfabeto ed il supporto usato non contano.

[269] In tal modo si favorirebbe dunque la riflessione e nel contempo si consentirebbe la documentazione: cioè le due finalità essenziali svolte dal documento scritto (così R. Borruso, *Computer e diritto - Tomo II, Profili giuridici dell'informatica*, cit., p. 218).

[270] E. Giannantonio, *op. cit.*, p. 385.

Conseguentemente, accogliendo tale nozione (ampia) di scrittura, si riconosceva che non soltanto i documenti elettronici in senso ampio, come i tabulati, ma anche i documenti elettronici in senso stretto[271], come i dischi, magnetici o ottici, potessero essere considerati documenti scritti: questo proprio perché essi consistono in una dichiarazione incorporata su un supporto materiale durevole. Il documento elettronico, infatti, contiene un messaggio in un linguaggio convenzionale (il linguaggio dei bit, il quale viene scritto con sistema binario, cioè un sistema matematico basato su due cifre: 1 e 0), su un supporto materiale mobile (che può essere un floppy disk, un hard disk, oppure un compact disk[272]) e destinato a durare nel tempo[273].

E non sembravano costituire impedimenti a tali conclusioni le obiezioni relative alla non immediata leggibilità dei documenti elettronici, ed alla necessità dell'uso dello stesso computer per una loro intelligibilità. A tale obiezione, infatti, si rispondeva rilevando come il requisito della «leggibilità ad occhio nudo» non potesse essere considerato necessario per ritenere l'atto scritto, perché altrimenti si sarebbe dovuto negare la stessa efficacia della forma scritta ad un documento solo perché redatto in caratteri microscopici, o in una lingua a noi non immediatamente comprensibile[274]. Ed inoltre nel nostro ordinamento non vi sono norme che richiedano l'immediata leggibilità di un determinato testo per considerarlo scritto, e quindi nessuna difficoltà sembrava esserci ad equiparare il documento reso su supporto cartaceo tradizionale con i più moderni documenti redatti attraverso le nuove tecnologie.

Ed anche le teorie sulla natura giuridica dei documenti informa-

[271] Sulla distinzione tra documenti elettronici in senso ampio e documenti elettronici in senso stretto si veda al paragrafo 210.

[272] Come già ricordato in altra parte del testo, rispettivamente un dischetto estraibile dal computer, un disco fisso facente in genere corpo con l'elaboratore, oppure un disco metallico a lettura ottica.

[273] Questo in tutti i casi in cui il documento è memorizzato in un sistema informatico: anche quando, dunque, si tratti di memorie circuitali RAM, di carattere sì volatile, ma pur sempre con una certa durata e con la possibilità di rintracciarne l'esistenza; e sicuramente nel caso di memorie ROM, destinate a mantenersi in forma inalterabile nel tempo, o di memorie di massa o ausiliarie magnetiche, le quali perdurano finché un intervento umano non provveda a cancellarle o modificarle, ad eccezione delle memorie ausiliarie di tipo ottico, che in linea di massima non sono modificabili una volta inciso il supporto mediante il raggio laser.

[274] Così F. Parisi, *Il contratto concluso mediante computer*, CEDAM, Padova 1987, p. 70.

tici che consideravano la forma elettronica come una «forma *dematerializzata*», né scritta né orale, che utilizza per la sua manifestazione gli impulsi elettronici e la cui percezione da parte dell'uomo è assicurata comunque in maniera tradizionale, o attraverso la scrittura (su video o su carta) o attraverso il linguaggio orale, concludevano in ogni caso per l'assimilazione allo scritto: questo sulla base del rilievo che tale forma «*dematerializzata*», in quanto veicolata da un impulso elettronico, partecipa comunque maggiormente dei caratteri dello scritto piuttosto che del linguaggio orale[275].

Un ultimo rilievo, suggello alle teorie degli studiosi di diritto dell'informatica appena riportate, riguardava una considerazione di natura maggiormente pratica, basata sulla situazione del diritto positivo.

Infatti, nel campo dei rapporti civili, non si aveva alcun dubbio che le norme sulla forma dei contratti e quelle sulla prova documentale avessero come presupposto la convinzione che lo scrivere consistesse nell'apporre dei segni grafici sulla carta; ma d'altro canto non esisteva alcuna disposizione che escludesse altri modi di scrivere e documentare. Il sistema appariva, quindi, già da allora aperto alle recenti innovazioni tecnologiche: occorreva solo convincersi che si sarebbe potuto scrivere anche registrando dati su una memoria magnetica. Ma, trattandosi comunque di una soluzione interpretativa, non venivano escluse numerose incertezze, oltre alle resistenze degli studiosi e degli operatori del diritto maggiormente legati alla tradizione e non a proprio agio con le nuove tecnologie.

Più vicina a queste posizioni «chiuse» si pose un'altra dottrina[276] che, con riferimento alla natura giuridica del documento informatico, tendeva ad assimilarlo ad una figura diversa dal documento scritto, quella delle *riproduzioni meccaniche e fotografiche*[277], il cui valore probatorio è disciplinato nel più volte ricordato art. 2712 del codice civile. Questo in quanto «l'amplissima dizione – in genere ogni rappresentazione meccanica di fatti – contenuta nell'articolo 2712 cod. civ. dimostra l'intenzione del legislatore di dettare in quell'articolo la disciplina di ogni strumento meccanico, pur non esistente al tempo della legge, per mezzo del quale siano riprodotti o anche posti in essere, contestualmente al medesimo strumento, idoneo a rappresentarli, fatti e perciò anche atti e in specie dichiarazioni giuridicamente rilevanti»[278].

[275] Così R. Clarizia, *Informatica e conclusione del contratto*, Giuffrè, Milano 1985, p. 175.

[276] In particolare L. Montesano, *Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Dir. Inf. Inf.*, 1987, p. 25; tale tesi risulta seguita anche da De Santis, *Il documento non scritto come prova civile*, Napoli 1988, p. 90 ss.

[277] Sulle riproduzioni meccaniche si vedano E. Massari, *Riproduzioni meccaniche, copie ed esperimenti (in materia civile)*, in *Noviss. Dig. it.*, XV, Torino 1968, p. 1244; Lucifero, *Riproduzioni meccaniche, copie ed esperimenti*, in *Enc. dir.*, XL, Milano 1989, p. 1081.

E nonostante che il termine «meccanico» fosse usato dal legislatore con un'accezione che non si conciliava con le modalità operative dell'elaboratore elettronico[279], e attraverso una lettura evolutiva delle disposizioni codicistiche[280], si giungeva all'affermazione che il documento informatico costituisse riproduzione meccanica quando l'attività di elaborazione non incidesse sugli elementi essenziali ai fini della rilevanza probatoria del fatto[281]. Invece, nel caso in cui l'oggetto della riproduzione fosse costituito da un documento scritto, si sarebbe rientrati nell'ambito di applicazione dell'art. 2719 cod. civ. e nell'ipotesi ivi prevista, quella cioè delle copie fotografiche di scritture.

Le diverse teorie esaminate, pur giungendo a conclusioni differenti, non devono necessariamente essere viste come alternative tra loro.

Infatti, la grande varietà che contraddistingue i documenti informatici comporta, come già ricordato in precedenza, che essi non possano essere considerati unitariamente, ma che di volta in volta occorra esaminare le caratteristiche del singolo documento al fine di individuarne la natura giuridica. In merito si osservi, inoltre, che dalla nozione di documento informatico accolta dal legislatore all'art. 491-*bis* c.p. risulta che il fatto documentato può essere costituito da dati o informazioni aventi efficacia probatoria, ovvero da programmi specificamente destinati ad elaborarli: pertanto il documento informatico può costituire sia un documento indiretto, e cioè un documento che ha come mezzo di rappresentazione la scrittura e che affida l'immagine del fatto all'espressione del pensiero di chi scrive (al pari delle

[278] L. Montesano, *Sul documento informatico*, cit., p. 25.

[279] E. Giannantonio, *Manuale di diritto dell'informatica*, cit., p. 379.

[280] Così B. Amory-Y. Poullet, *Le droit de la preuve face a l'information et a la telematique*, in *Rev. int. dir. comp.*, 1985, p. 341; nello stesso senso Verde, *Per la chiarezza di idee in tema di documentazione informatica*, in *Rivista di diritto processuale*, 1990, p. 727.

[281] E. Giannantonio, *op. ult. cit.*, p. 379.

altre scritture e delle riproduzioni cartografiche); sia un documento diretto, e cioè un documento che permette una percezione immediata del fatto, ponendo l'interprete direttamente di fronte allo stesso per mezzo dell'ausilio di apparecchiature tecniche (al pari dei documenti fotografici, fonografici o cinematografici).

In base alla prima delle due ipotesi prospettate, esaminata quando è stata approfondita l'analisi del documento informatico di carattere dichiarativo, consegue la possibile assimilazione della nuova «*res*» rappresentativa al documento scritto. Viceversa, nel caso in cui i documenti informatici costituiscano la riproduzione di fatti esterni o di altri documenti, sembrerebbe potersi ipotizzare l'applicazione delle norme previste dagli artt. 2712 e 2719 c.c. in tema di riproduzioni meccaniche e di copie fotografiche di scritture[282].

Il rapporto tra le diverse fattispecie può essere analizzato anche con riferimento alle caratteristiche del contenuto del documento informatico. Infatti, nel caso in cui esso riproduca una preesistente realtà, si applicherebbe l'art. 2712 quando la riproduzione del documento informatico riguarda un fenomeno o una cosa in genere; al contrario, quando tale tipo di documento riproduce specificamente un precedente documento scritto, l'articolo del codice che dovrebbe applicarsi è il 2719[283]. Nel caso in cui la «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» non si riferisca a realtà preesistenti, ma venga formata direttamente attraverso l'uso del sistema informatico, si rientrerebbe, invece, nell'ambito delle teorie che concepiscono il documento informatico quale documento scritto.

[282] Deve tuttavia ribadirsi che, pur potendo la riproduzione avere ad oggetto il fatto di una dichiarazione, l'applicabilità dei citati articoli risulta esclusa ogni qualvolta il fatto della dichiarazione debba essere documentato in maniera tipica: e ciò in conseguenza di quanto sopra osservato ed in ragione della funzione residuale ricoperta dalle menzionate norme rispetto a quella propria dell'art. 2702 c.c.

[283] Così E. Giannantonio, *op. ult. cit.*, p. 383, che però esclude da tale dicotomia il documento riprodotto mediante apparecchiatura *telefax*, per il quale, nonostante l'orientamento giurisprudenziale riportato, sembra preferire l'applicazione dell'art. 2719 c.c. Sul valore probatorio dei documenti trasmessi mediante *telefax* si veda anche V. Frosini, *Il telefax e il diritto*, in *Poste e telecomunicazioni*, a. LVIII, n. 1, 1990, pp. 62 e ss., C. Barreca, *Telex e telefax nel sistema delle prove documentali*, nota a Cass., 13/2/1989 n. 886, in *Riv. dir. proc.*, 1991, II, pp. 907 ss.;. M. Bronzini, *Il telefax nella gestione delle procedure concorsuali*, in *Dir. fall. e soc. comm.*, 1991, I, pp. 1008 ss.; L. Grisostomi Travaglini, *Esclusione da una gara di appalto per presentazione di documenti mediante fax*, nota a TAR Lazio 27/11/1990 n. 2130, in *Dir. Inf. Inf.*, 1991, pp. 909 ss.

Stabilita, quindi, la natura giuridica del fenomeno in esame, nel prossimo paragrafo si analizzerà quale valore giuridico la dottrina era giunta ad attribuirgli in assenza di un suo riconoscimento normativo[284], per poi verificare le scelte interpretative adottate alla luce della disciplina legislativa del sistema di validazione giuridica dei documenti informatici, in particolare quello delle firme elettroniche e/o digitali: sistema in particolare che ha questa volta esplicitamente affermato sia la natura giuridica del documento informatico, sia il suo valore normativo, come si vedrà oltre nel testo.

212. *Il valore giuridico del documento informatico.* – Una volta accertato, anche se essenzialmente in base all'interpretazione ed agli studi degli esperti del diritto dell'informatica, che il documento elettronico può essere considerato un documento scritto, e nello stesso tempo, o in alternativa, una riproduzione meccanica o la copia fotografica di scritture, appare ora necessario ricostruire quale valore giuridico gli era stato in passato assegnato.

Innanzitutto occorre, però, chiarire che, anche nel caso del documento informatico, per potergli attribuire efficacia giuridica, si deve preventivamente accertare la sua genuinità e sicurezza[285]. La mancanza di genuinità, in tale specifica ipotesi, può derivare da diverse cause connesse ai vari momenti del processo di elaborazione: durante la fase di acquisizione delle informazioni, al momento della loro elaborazione, oppure durante la loro trasmissione. A prescindere dai motivi che provocano tali alterazioni, tecnici o dipendenti dall'intervento dell'uomo, intenzionali o meno, una particolare attenzione deve essere portata ai metodi per evitarli, e quindi ai sistemi di sicurezza dei dati. Tra questi, collegati essenzialmente alle stesse informazioni (e quindi non agli apparati meccanici che compongono il sistema informatico), rivestono particolare importanza le tecniche crittografiche:

[284] Indagine che, alla luce delle probabili difficoltà che si incontreranno nella gestione dei documenti informatici secondo i requisiti richiesti dal D.P.R. 445/2000, e dal suo Regolamento tecnico approvato con D.P.C.M. 8 febbraio 1999, potrà risultare estremamente utile anche oggi, nonostante l'introduzione del sistema della firma digitale: si eviterebbe, infatti, di lasciare senza tutela quei documenti che non rispettano i citati requisiti. Sul punto si veda comunque anche oltre, nei prossimi paragrafi.

[285] 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.

tecniche che rendono i dati e i programmi inintelligibili a chi non conosca l'opportuna chiave e l'algoritmo di trasformazione, come si vedrà in maniera particolareggiata nelle prossime pagine.

Tornando, invece, al tema del valore giuridico del documento elettronico, analizzato attraverso un esame delle teorie che si sono succedute nel tempo, le diverse tesi della dottrina si sono orientate su due posizioni: quella che dava della legge un'interpretazione funzionalistica, che verificava quindi il rispetto degli obiettivi perseguiti dalle norme, perché questi ultimi potevano, col tempo, rivelarsi sorpassati, o non più gli unici che rendessero possibile in concreto adeguarsi al diritto positivo; o quella che ne dava un'interpretazione formalistica, che attribuiva alla lettera della norma un contenuto ed una portata sostanziali, considerandola, quindi, come la manifestazione di una precisa volontà legislativa, senza possibilità di interpretarla diversamente da come era stata resa e dalle parole adoperate.

Sulla base della seconda posizione[286], pur attribuendo la natura di documento scritto al documento informatico, abbastanza pacificamente si ritenne che le «rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti» non potessero essere assimilabili né all'atto pubblico, almeno a quello in senso stretto[287], né alle scritture private: nel primo caso per l'impossibilità di rendere in formato elettronico le formalità previste dalla legge, richiamate nell'art. 2699 del

[286] In particolare si veda E. Giannantonio, *Manuale di diritto dell'informatica*, cit., p. 389 e ss., e R. Borruso, *Computer e diritto,* II, cit., p. 216 e ss..

[287] Secondo la prevalente dottrina, il concetto di «documento pubblico» è individuato esclusivamente con riferimento al soggetto dal quale proviene, e quindi dal pubblico ufficiale o dal pubblico impiegato, ed è tendenzialmente coincidente con quello di atto pubblico in senso ampio (categoria che quindi comprende non soltanto gli atti emessi dalla Pubblica Amministrazione, ma tutti gli atti emessi dai pubblici uffici: si veda a tale proposito A.M. Sandulli, *Documento - Diritto amministrativo*, in *Enc. dir.*, XIII, Milano 1964, p. 607; M.S. Giannini, *Documentazione amministrativa*, in *Enc. dir.*, XIII, Milano 1964, p. 596; G. Bertola, *Documentazione amministrativa*, in *Noviss. Dig. it.*, VI, Torino, p. 75; E. Morone, *Documentazione amministrativa, autenticazione e legalizzazione di firme*, in *App. Noviss. Dig. it.*, III, Torino, p. 118). Atto pubblico in senso stretto è invece quello disciplinato nell'art. 2699 del codice civile, che lo definisce come quel «documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato» (la distinzione è riportata da E. Giannantonio, *Manuale di diritto dell'informatica*, cit., p. 349; sugli atti pubblici in particolare si vedano: G. Crisci, *Atto pubblico (Diritto civile)*, in *Enc. dir.*, IV, Milano, p. 265; B. Brugi-M. Dossetto, *Atti pubblici*, in *Noviss. Dig. it.*, I, Torino, p. 1521; A. Morello-E. Ferrari-A. Sorgato, *L'atto notarile*, Milano 1977).

codice civile, e la sottoscrizione del pubblico ufficiale, requisito richiesto tradizionalmente autografo[288]. Con riferimento alle scritture private, essenzialmente per l'impossibilità di accettare una sottoscrizione non apposta di propria mano dal dichiarante[289].

Sembrava, quindi, doversi conferire al documento elettronico un valore giuridico residuale, quello della riproduzione meccanica o fotografica, richiamato dall'art. 2712 c.c., oppure quello delle copie fotografiche di scritture, disciplinato nell'art. 2719 c.c. Fatto comunque sempre salvo il principio del libero convincimento del giudice sul ter-

[288] Le formalità di redazione di tali documenti risultavano fissate dalla legge 4 gennaio 1968, n. 15, il cui art. 12 (dal titolo «Redazione di atti pubblici») disponeva che «le leggi, i decreti, gli atti ricevuti dai notai e tutti gli altri atti pubblici sono redatti a stampa, o con scrittura a mano o a macchina»: il Legislatore pertanto, nell'introdurre positivamente il principio della necessità della forma scritta degli atti pubblici, si riferiva alla tradizionale nozione di scrittura, presupponendo cioè la consistenza cartacea di tali atti. Su tale costrutto sono intervenute le recenti novità in materia di validazione giuridica della documentazione informatica, novità che portano a rivedere quella che era la concezione tradizionale cartacea del documento: oggi sia il documento, sia la scrittura, vengono concepite in maniera più ampia, comprendente anche le nuove metodologie informatiche e telematiche. Così, la l. 15/1968 è stata espressamente abrogata dal D.P.R. 28 dicembre 2000 n. 445, che però ne ha ripreso la disciplina aggiornandola: in particolare, l'art. 12 citato è stato riportato nel suo art. 7, il cui primo comma dispone che «i decreti, gli atti ricevuti dai notai, tutti gli altri atti pubblici, e le certificazioni sono redatti, *anche promiscuamente, con qualunque mezzo idoneo*, atto a garantirne la conservazione nel tempo»: nessun legame quindi ad un supporto o ad un metodo, seppur «tradizionale» (nella specie quello cartaceo), ma un'apertura a qualunque tecnica adeguata al fine della comunicazione e della conservazione nel tempo. Occorre però richiamare anche il disposto della legge 16 febbraio 1913, n. 89, sempre in materia di «confezione» di atti pubblici, che, tra l'altro, espressamente prevede la necessità della sottoscrizione del documento ad opera del notaio e delle altre parti (art. 51): requisito che sembrava non potersi soddisfare usando esclusivamente un sistema informatico per la redazione dell'atto da parte del notaio.

[289] Con riferimento alla disciplina della scrittura privata, il codice civile non ne enuncia la definizione, limitandosi a regolarne la fattispecie agli artt. 2702-2708. In particolare, gli elementi che compongono il documento in esame sono rappresentati dalla cosa su cui è impressa la scrittura, dalla scrittura medesima e dalla sottoscrizione. Tra questi requisiti è la sottoscrizione che assume maggiore rilievo, costituendo il mezzo adottato dall'ordinamento per imputare ad un determinato soggetto la paternità del documento («Essa è il criterio di imputazione, onde il diritto attribuisce a taluno, come suo autore, un testo grafico (...) L'esigenza, soddisfatta dalla firma autografa, sta nella personalità ed esclusività del rapporto tra autore e testo: la firma è di lui, e non può essere di altri»: così N. Irti, *Idola libertatis. Tre esercizi sul formalismo giuridico*, Milano 1985, p. 24).

reno della valutazione delle prove, stabilito nell'art. 116 del codice di procedura civile.

Con tale costrutto interpretativo ad opera della prevalente dottrina andarono a scontrarsi diverse tesi, caratterizzate da una maggiore apertura alle nuove forme e metodologie di documentazione, e ad un'assimilazione delle stesse anche a costruzioni giuridiche più importanti, in particolare a quella della scrittura privata.

Così, deve ricordarsi quella dottrina che più in generale, e non solo quindi con riferimento al tema in esame, rilevava una «crisi della sottoscrizione» quale criterio esclusivo di imputazione della provenienza delle dichiarazioni[290], e quindi quale unico elemento per considerare un determinato documento «scrittura privata» ai sensi dell'art. 2702 c.c.; mentre riteneva che potesse anche essere utilizzato, in alternativa ed oltre agli altri casi già previsti dal diritto positivo (come il telegramma non sottoscritto, ex art. 2705 c.c., o i titoli di credito pubblici con la firma stampigliata secondo l'art. 5 del R.D. 11 febbraio 1911, n. 298), il principio dell'esclusività dell'uso dell'apparato tecnico[291]. Né devono essere ignorati i tentativi di interpretazione delle

[290] Sulla base di un'attenta osservazione del mondo dell'«aformalismo della macroeconomia», tale dottrina sottolineava l'importanza assunta nel nostro tempo dai beni mobili e dal relativo commercio, e quindi sottolineava che «i negozi più rilevanti si risolvono in accordi *comunque espressi*» a prescindere dal requisito della sottoscrizione, per poi concludere (anche in seguito all'esame della disciplina legislativa e della dottrina) rilevando una «profonda lacerazione» del nesso tra scrittura privata e firma autografa. È infatti il graduale scioglimento del rapporto tra firma autografa e testo scritto, insieme al già ricordato progressivo e sempre più comune uso delle nuove tecnologie per la redazione dei documenti e per la comunicazione degli stessi, al ritmo intenso degli affari e alla distanza tra i soggetti comunicanti (oggi il mercato è globale), che determina «l'espansione dell'attività documentatrice (non parole dette, ma parole scritte) e la crisi della firma autografa»: processo destinato ad accelerarsi ed intensificarsi proporzionalmente all'espansione dell'utilizzo delle indicate tecnologie (N. Irti, *op. cit.*, p. 25 e 75). Sulle ragioni del declino progressivo della firma autografa, vedi il § 29 del libro citato in prefazione. Il requisito della sottoscrizione, dunque, storicamente legato al contratto tra persone presenti ed all'uso sociale delle lettere missive, si scopre oramai incompatibile con le moderne tecniche di fissazione e trasmissione della parola. Si deve invece pensare a nuovi metodi di imputazione della dichiarazione, come ad esempio quello dell'uso esclusivo dell'apparato tecnico. E l'esortazione di tale autore ad «una pronta ed accorta disciplina legislativa» al fine di «prevenire le tortuose strade dell'analogia e le arditezze della giurisprudenza» sembrano essere state raccolte proprio dalla normativa in materia di firma digitale, come si vedrà oltre nel testo.

[291] Così N. Irti, *op. cit.*, p. 28.

norme esistenti in materia di forma in un'ottica «funzionalistica», consentendo, quindi, la verifica dell'adeguatezza della forma elettronica a soddisfare le finalità e le esigenze richieste per la sottoscrizione dalle norme in materia di scrittura privata[292]. Tenendo tra l'altro presente che «qualunque sia il materiale utilizzato per dire, dichiarare, manifestare, comunicare, trasmettere un dato messaggio, se questo contiene un regolamento negoziale giuridicamente rilevante appare evidente che anche l'elettronica, la telematica e gli apparati magnetici danno un consistente contributo alla creazione di situazioni di fatto non immeritevoli di tutela giuridica»[293].

Non si devono poi dimenticare le ipotesi, riportate nel paragrafo precedente, che considerano il documento informatico come riproduzione meccanica o copia fotografica di scrittura, ed occorre quindi esaminare come debba essere concepito il suo valore giuridico nelle due fattispecie.

Secondo tale orientamento, al documento informatico poteva essere attribuita, quale conseguenza della sua assimilazione alle riproduzioni meccaniche o alle copie fotografiche, un'efficacia probatoria condizionata al mancato disconoscimento di colui contro il quale sono prodotte, ed analoga a quella stabilita per la scrittura privata dagli artt. 2702 e 2703 c.c.[294]. Nell'ipotesi disciplinata dall'art. 2712 c.c., o in quella dell'art. 2719 c.c., non sono tuttavia previsti, contrariamente a quanto disposto per la scrittura privata, termini di decadenza o forme particolari per il disconoscimento, essendo sufficiente a tal fine una dichiarazione che neghi la conformità della riproduzione ai fatti da documentare[295]. Pertanto il documento elettronico non disconosciuto forma piena prova dei fatti o delle cose rappresentate non potendo il giudice «porre a base della propria decisione la rappresentazione di fatti o di cose che diverga dalla rappresentazione dei medesimi, espressa nella riproduzione meccanica esibita», né disporre una consulenza tecnica o un esperimento tecnico ex art. 216 c.p.c. in or-

[292] R. Clarizia, *Informatica e conclusione del contratto*, cit., p. 175.

[293] Così F. Stallone, *La forma dell'atto giuridico elettronico*, in *Contratto e impresa*, 1990, p. 576.

[294] In tal senso per primo F. Carnelutti, *Prova fotografica e fonografica*, in *Riv. dir. proc. civ.*, 1942, I, p. 233.

[295] In tal senso Cass., 22 maggio 1982, n. 3143, in *Giur. it.*, 1983, I, p. 968, con nota di F. Trifone; Cass., 17 giugno 1985, n. 3652, in *Giust. civ.*, 1986, p. 2535, con nota di S. Russo.

dine all'attendibilità della riproduzione[296]; il documento informatico disconosciuto, invece, non solo non avrebbe potuto costituire piena prova, ma non avrebbe potuto neppure essere considerato dal giudice prova sufficiente in base al suo prudente apprezzamento, risultando necessario che la parte che intendesse valersene ne chiedesse la verificazione proponendo i mezzi di prova che ritiene a questo fine utili, ed in particolare consulenze o esperimenti tecnici ex art. 261 c.p.c.[297].

Qualche elemento di novità nella teoretica sul valore giuridico del documento elettronico venne poi portata da una «leggina» dettata specificamente per la fattispecie della comunicazione delle parti nel processo, in particolare quella degli avvocati, e per questo motivo non molto considerata: ci si riferisce alla legge 7 giugno 1993 n. 183, sull'utilizzazione dei mezzi di telecomunicazione per la trasmissione degli atti relativi a procedimenti giurisdizionali[298]. Anche se in una materia specifica e legata più al diritto processuale che al diritto sostanziale, in tale norma si afferma un primo riconoscimento sia del documento informatico, sia del suo valore giuridico; e si conferma (almeno parzialmente) che la necessità dell'autografia della sottoscrizione non è requisito essenziale per attribuire un valore allo stesso documento[299].

[296] V. Andrioli, *Diritto Processuale Civile*, I, Napoli 1979, p. 695.

[297] Così L. Montesano, *Sul documento informatico*, cit., p. 27.

[298] Nel caso ricorra quest'ultimo requisito, si considera conforme all'originale anche la copia teletrasmessa di provvedimenti del processo, ovvero di atti o provvedimenti relativi ad altri procedimenti.

[299] Tale legge prevede la possibilità per l'avvocato di trasmettere «attraverso mezzi di telecomunicazione» (e quindi anche mediante sistemi di posta elettronica) la copia di un atto del processo ad altro avvocato o procuratore, *copia che si considera conforme all'originale* se entrambi i legali siano muniti di procura ex art. 83 c.p.c. (procura che può risultare anche dall'atto trasmesso), l'atto sia sottoscritto in maniera leggibile da parte del procuratore trasmittente, la copia ricevuta sia sottoscritta per la conferma dal procuratore ricevente. Per un commento a questa disciplina, e per una sua applicazione ai nuovi strumenti informatici e telematici si veda G. Ciacci-P. Varì, *Forme alternative di notificazione: la notifica mediante strumenti informatici*, in *Rivista di Diritto Commerciale*, Padova 1994, 1/2, pp. 95-132. Collegata a tale disciplina, e tra l'altro sempre in materia processuale, è anche la legge 21 gennaio 1994 n. 53, intitolata «Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali», su cui si veda ancora G. Ciacci, *Comunicazioni e notificazioni di atti processuali in forma elettronica*, in *La tecnologia dell'informazione e della comunicazione in Italia. Rapporto FTI 1996*, Franco Angeli, Milano 1997, pp. 262-282; G. Costantino, *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.

Ulteriore costruzione dottrinaria in materia che deve essere segnalata, nell'ambito di questa specie di *excursus* storico relativo alle posizioni degli operatori del diritto sul valore giuridico del documento elettronico, e rinviando ai prossimi paragrafi l'esame delle novità apportate alla materia dall'introduzione nel nostro ordinamento del sistema della firme elettroniche e digitali, è quella successiva all'introduzione della disciplina delle falsità di documenti informatici, come prevista dalla già ricordata legge 23 dicembre 1993 n. 547.

Tale legge consente una nuova concezione del documento prodotto dall'elaboratore elettronico, come categoria generale la cui importanza va bene al di là del trattamento penalistico che l'art. 491-*bis* c. p. riserva alle sue falsificazioni: infatti, se il documento informatico è fatto oggetto, in quanto tale, di tutela penale, «esso deve essere riconosciuto come esistente ed efficace anche in tutti gli altri campi del diritto»[300]. E, tra l'altro, con un valore giuridico tutt'altro che residuale, poiché la registrazione in *bit* è assimilata dal legislatore alla scrittura, spiegandosi in questo modo la sussunzione delle falsità commesse nei documenti informatici tra quelle commesse negli atti pubblici o nelle scritture private[301]: «scrittura come quella autografa o dattiloscritta o a stampa di atti che, indipendentemente da tale forma (e quindi anche da quella elettronica), continuano ad essere pubblici o privati a seconda di come siano rogati»[302]. Anche se poi, più pru-

[300] Tale interessante teoria, elaborata ben prima dello sviluppo di un sistema di firma digitale sulla base della crittografia asimmetrica come quello introdotto nel nostro Paese dal D.P.R. 513/1997 ed oggi disciplinato dal D.P.R. 445/2000, è riportata in R. Borruso, *La tutela del documento e dei dati*, in Aa.Vv., *Profili penali dell'informatica*, cit., p. 13.

[301] Si ricordi, infatti, che l'art. 491-*bis* usa una formula molto chiara nel disporre (nel comma I) che «*se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*».

[302] Così sempre R. Borruso, *op. cit.*, p. 13, che però, dopo aver con forza affermato, in linea con quanto sostenuto da tempo in suoi precedenti scritti, l'assimilazione della registrazione dei *bit* alla scrittura, al momento di attribuire a tale registrazione un valore probatorio, si arresta di fronte all'ostacolo dell'autografia della sottoscrizione: e, sulla considerazione che la nozione indicata di documento informatico debba essere considerata una «norma in bianco» da riempirsi mediante rinvio ad altre discipline, afferma che l'art. 491-*bis* riconosce sì l'esistenza di tale nuova cosa rappresentativa di un fatto, ma per tutelare penalisticamente quelle alle quali

dentemente ed in tempi non ancora «maturi», la dottrina a commento della disciplina introdotta dalla l. 547/1993 preferì acquisire la nuova rilevanza del documento informatico, e rinviare ad altri settori dell'ordinamento l'indagine circa il suo valore probatorio[303].

Quanto esposto fino ad ora relativamente alle varie teorie dottrinarie che, nonostante si dovessero confrontare con un apparato legislativo carente in materia di documentazione prodotta e gestita attraverso l'informatica (e comunicata a distanza grazie alla telematica), erano comunque riuscite a ricostruire la natura ed il valore giuridico della «*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*», deve essere rivisto alla luce dell'introduzione, nel nostro ordinamento giuridico, di un sistema di validazione giuridica del documento elettronico basato sulla firma digitale e su quella elettronica.

213. *Firma elettronica, firma digitale e valore giuridico del documento elettronico.* – Nel 1997 il nostro Paese, che fino a quel momento non si era mai distinto per il livello di interesse verso le nuove tecnologie, soprattutto prendendo in considerazione la loro regolamentazione normativa[304], si poneva improvvisamente ai primi posti tra quelli maggiormente informatizzati nel settore del riconoscimento giuridico della documentazione elettronica: risolvendo in questo modo molte delle difficoltà che si erano incontrate nel dare un fondamento ed una sicurezza giuridica all'attività di documentazione svolta attraverso il computer.

Prima l'art. 15, comma 2, della legge 15 marzo 1997 n. 59 (in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici), poi il D.P.R. 10 novembre 1997 n. 513 (il regolamento di attuazione del citato art. 15, che ha introdotto in Italia il sistema della firma digitale), si distinguevano per la

vada riconosciuta efficacia probatoria in base ad altre leggi (R. Borruso, *op. cit.*, pp. 14 e 16).

[303] Si veda anche P. Galdieri, *op. cit.*, p. 111.

[304] Le principali leggi emanate fino a quell'anno, infatti (e comunque dopo un lungo periodo di vuoto normativo collegato ad una realtà tecnologica in costante espansione ed evoluzione), erano state in genere diretta conseguenza di una produzione comunitaria, e quindi adempimento dei rispettivi obblighi (tra esse si possono ricordare il D.Lgs 29 dicembre 1992 n. 518 in materia di tutela del software, la l. 23 dicembre 1993 n. 547 sui crimini informatici, e la l. 31 dicembre 1996 n. 675 in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali).

loro articolata organicità nel disciplinare l'uso dell'elaboratore elettronico nell'attività documentale della pubblica amministrazione e dei privati: attività che si poteva concretizzare nella redazione di contratti, nella comunicazione a distanza attraverso la telematica, nei pagamenti elettronici, nella possibilità di formare e conservare su supporti informatici libri, repertori e scritture di cui fosse obbligatoria la tenuta. In nessun altro Paese tra quelli tecnologicamente avanzati poteva riscontrarsi a quel momento una normativa così completa e progredita dal punto di vista tecnologico e da quello sistematico-giuridico[305]: l'uso della funzione di *hash* insieme alla crittografia asimmetrica per apporre la c.d. firma digitale da una parte, il riconoscimento della natura giuridica di documento scritto e del valore giuridico della scrittura privata o della riproduzione meccanica al documento informatico con tale nuova forma di «sottoscrizione» informatica dall'altra[306], rappresentavano una vera e propria «rivoluzione» nella tradizione dell'attività di documentazione (quella essenzialmente cartacea e con sottoscrizione autografa)[307].

[305] Si registravano produzioni in materia in alcuni Paesi degli Stati Uniti d'America (Utah, Illinois, Florida, Washington), in Germania ed a Singapore, ma in tutti i casi venivano previste tecnologie per ottenere la certezza della provenienza e non ripudiabilità dei documenti informatici non così complete, mentre si consideravano conseguenze giuridiche non così pregnanti.

[306] Sia per ciò che riguarda i concetti di «*hash*» e «crittografia asimmetrica», sia per gli aspetti legati al valore probatorio del documento elettronico, si veda più avanti nel testo.

[307] A tale originale produzione purtroppo non seguì, negli anni successivi, una pari attenzione delle istituzioni, e soprattutto degli utenti (privati o operatori economici), per l'attuazione del sistema. Nonostante infatti i rilevanti vantaggi conseguenti alla realizzazione del disposto normativo, non ultimi quelli di fare acquisire certezza a settori nuovi e in costante espansione (si pensi al mercato del commercio elettronico su Internet), si registrarono posizioni di netta avversione nei confronti dell'innovativo sistema, sorrette spesso da argomentazioni giuridiche non totalmente fondate (in genere il sistema veniva sottoposto a forti critiche usando parametri e requisiti molto più rigidi di quelli normalmente utilizzati per la corrispondente attività di documentazione nella tradizionale forma cartacea, sorrette tra l'altro da fondamenti tecnici spesso non corretti: si pensi, ad esempio, alla lunga polemica ed alle difficoltà relative alla verifica della funzione del titolare del dispositivo di firma elettronica, problema sollevato con riferimento all'attività di autenticazione, ma solo con riferimento a quella digitale). Questo fatto, insieme alle lungaggini tipiche della realtà della pubblica amministrazione, chiamata ad un passaggio culturale ed organizzativo estremamente complesso, ed alla scarsa familiarità con i nuovi strumenti da parte dei privati, hanno portato ad una lentissima attivazione del sistema della firma digitale, tranne rare e sporadiche, seppur importanti, eccezioni.

Per meglio capire comunque la rivoluzionaria innovazione di cui si è appena parlato, e quindi per giungere a utilizzare in maniera consapevole e con pieno valore giuridico il computer per l'attività di documentazione da parte dei privati e della pubblica amministrazione, si esporranno ora le caratteristiche principali del sistema italiano di firma digitale, questo alla luce delle novità recentemente introdotte dal D.Lgs. 23 gennaio 2002 n. 10 (che ha recepito la Direttiva comunitaria 1999/93/CE in materia di firme elettroniche, introducendo questa figura anche nel nostro Paese), incominciando dalla descrizione semplificata della tecnologia coinvolta.

214. *La firma digitale e la firma elettronica da un punto di vista tecnico.* – Per ottenere il risultato di assicurare la genuinità e la sicurezza dei documenti prodotti attraverso l'uso dell'elaboratore elettronico (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, l'alterazione è facile da accertare e da ricostruire), genuinità che nell'attività documentale informatica è minacciata da diversi fattori[308], sono state adottate soluzioni basate sulla crittografia.

La «crittografia» è quella 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 possiedano la chiave segreta di decifrazione. La funzione è infatti reversibile, per cui l'applicazione dello stesso algoritmo e della chiave segreta al testo cifrato restituisce il testo originale[309].

[308] Fattori che possono essere umani o tecnici, che coinvolgono i documenti elettronici sia nel momento della loro conservazione, che in quello della loro eventuale trasmissione a distanza.

[309] Di per sé la crittografia non è una novità. I procedimenti di cifratura esistono fin dall'antichità e, come l'etimologia del termine dimostra («crittografia», dal greco crupto, significa nascondere), 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*» usata per le comunicazioni tra i magistrati di Sparta e Lisandro, descritta da Plutarco nella sua opera *Vite parallele*; 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 alfabetico (questa volta la testimonianza è di Svetonio, nella *Vita dei Cesari*); dai banchieri fiorentini del Medio-evo, 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. Su tali notizie storiche si veda P. Ridolfi, *Dalla «scitala» di Plutarco alla firma digitale*, in *Media duemila*, ottobre 1998, p. 9, e, dello stesso autore, *Firma digitale e sicurezza informatica*, Franco Angeli, Milano 1998, pp. 1-128. Gli esempi indicati, ed in particolare l'ultimo, mostrano come le tecniche di crittografia siano state applicate soprattutto per soddisfare le esigenze di segretezza delle informazioni trattate in ambito militare e diplomatico. Ma anche in questo caso, con l'avvento e lo sviluppo di Internet quale nuovo *media* di informazione e comunicazione, la crittografia è definitivamente uscita 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 190 Paesi diversi del mondo, e per diverse ed ulteriori finalità, quali ad esempio quelle commerciali (oggi le comunicazioni che coinvolgono attività di *e-commerce*, come per i pagamenti *on line*, sono in genere sempre crittografate).

La crittografia può essere basata su due diversi sistemi. Il primo metodo, adatto soprattutto per soddisfare l'esigenza di genuinità del documento nel momento della sua conservazione «statica», cioè a prescindere da una sua comunicazione o trasmissione, utilizza la medesima chiave per criptare (prima) e per decriptare (poi) i messaggi. Si parla in merito di sistema *simmetrico* di criptazione, o a chiave segreta. Il problema di fondo che sorge con la sua utilizzazione è rappresentato dalla gestione delle chiavi quando si rende necessario trasmettere il documento a distanza, e quindi in una fase «dinamica» di attività, 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. Inoltre, nel caso di comunicazione con diversi soggetti, si ha la necessità di adottare chiavi diverse per ognuno di loro: sistema non più possibile nel momento in cui i soggetti non sono conoscibili preventivamente o sono molto numerosi[310]. Infine, altro aspetto negativo 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 criptazione, possono entrambe modificare o alterare il documento originario[311].

[310] Si pensi alla realtà resa possibile da Internet, ed in particolare alle applicazioni di commercio elettronico: in tal caso i soggetti che intraprendono relazioni commerciali e giuridiche vengono in contatto spesso per la prima volta direttamente sulla Rete, magari appartenendo a Paesi geograficamente molto lontani tra loro, e quindi non hanno la possibilità di scambiarsi in via preventiva, o comunque in sicurezza, l'unica chiave di criptazione.

[311] Possibilità che rende inutile l'uso di sistemi a chiave simmetrica per attribuire certezza giuridica alle dichiarazioni rese dalle parti di un determinato rapporto:

Proprio al fine di risolvere questi problemi di gestione della chiave, nel 1976 vennero inventati i sistemi *asimmetrici* di criptazione, detti anche *sistemi a chiave pubblica*[312]. L'algoritmo matematico richiede in questo caso l'applicazione di entrambe le chiavi al documento, seppure con finalità diverse (una per la criptazione, cioè per rendere illegibile il documento, l'altra per la decriptazione, cioè per l'operazione inversa). In tale ipotesi ciascuna persona risulta in possesso quindi di due chiavi, di cui una viene diffusa quanto più possibile e con diversi mezzi, e viene perciò detta «pubblica», mentre l'altra deve essere gelosamente custodita dal suo titolare, chiamata dunque «privata»[313]. La necessità per le parti di scambiarsi informazioni riservate relative al metodo di protezione del documento è eliminata in radice: come si è detto nella specie, infatti, la chiave privata è destinata a rimanere segreta ed è utilizzabile dal solo legittimo titolare; la chiave pubblica deve, invece, essere resa conoscibile con i più diversi mezzi (ad esempio mediante l'inserimento in archivi consultabili anche *on line*), associandola al nome di un titolare[314], e quindi la sua eventuale apprensione da parte di un terzo non è dannosa, ma connaturata allo stesso sistema.

La crittografia asimmetrica è suscettibile di due distinte applicazioni, potendo essere utilizzata a fini di segretezza, cioè per consentire la riservatezza delle comunicazioni telematiche, ovvero a scopo di autenticazione, cioè per garantire al destinatario di un messaggio digitale la certezza dell'identità del mittente, finalità che rileva in questa sede.

Nella prima ipotesi, crittografia asimmetrica *a fini di segretezza*,

si pensi, ad esempio, alla proposta ed all'accettazione trasmesse via posta elettronica in una vendita *on line*, che potrebbero essere modificate secondo le proprie esigenze da ciascuna delle parti.

[312] Tali sistemi, inventati da Whitfield Diffie e Martin Hellman e resi operativi l'anno dopo sotto il nome di RSA (acronimo delle iniziali dei suoi inventori, Rivest, Shamir e Adleman, tre scienziati del *Massachussets Institute of Technology* di Boston), sono detti «asimmetrici» perché la chiave di codifica e quella di decodifica sono completamente diverse (e quindi non simmetriche) e non ricavabili le une dalle altre.

[313] Per regola tecnica del sistema, il documento criptato dalla chiave pubblica di Tizio può essere decriptato solo dalla corrispondente chiave privata di Tizio, e viceversa.

[314] Garante di questa associazione, come si vedrà oltre, è il Certificatore, il soggetto che svolge proprio questa funzione mediante il rilascio di un certificato che deve essere allegato alla chiave pubblica.

A, intendendo inviare un messaggio riservato a B, in primo luogo si procura la chiave pubblica dello stesso B (o perché gli viene da lui fornita, oppure perché la acquisisce ricercandola negli appositi elenchi disponibili anche *on line*), e quindi cripta il messaggio utilizzando tale chiave; invia poi il messaggio criptato (come tale non comprensibile da alcuno) a B che, ricevutolo, per decriptarlo e quindi leggerlo, applica la propria chiave privata (di cui ha esclusiva gestione). In sintesi, il mittente cripta il messaggio con la chiave pubblica del destinatario, mentre quest'ultimo, e solo quest'ultimo, decripta il messaggio impiegando la (propria) chiave privata. Un qualsiasi soggetto che intercettasse il messaggio, non potendo utilizzare la chiave privata di B, non avrà alcuna possibilità di leggerne il testo[315].

Nella seconda ipotesi invece, quella della crittografia asimmetrica *a fini di autenticazione*, 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, volendo inviare a B un messaggio (senza necessità di soddisfare requisiti di segretezza, ma volendo assumersene la paternità), applica la propria chiave privata al suo testo, in questo modo «firmandolo elettronicamente», e lo spedisce; B, ricevuto il messaggio, applica al testo criptato la chiave pubblica di A (prelevata magari da un archivio telematico 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 (assioma fondamentale di tale sistema crittografico), la quale si presume sia di esclusiva conoscenza e disponibilità dello stesso A, B avrà la certezza che il messaggio proviene da A, mentre A non può efficacemente sostenere di non averlo criptato e quindi inviato.

Evidenti risultano i vantaggi dei sistemi a chiave pubblica rispetto a quelli simmetrici. In primo luogo, eliminata la necessità di trasmissione della chiave segreta (si ricordi che in questo caso non vi è proprio l'esigenza di inviare tale chiave per decriptare il testo), con i primi si realizza un maggior grado di sicurezza. In secondo luogo, sono i soli sistemi asimmetrici a consentire l'accertamento dell'impu-

[315] Infatti, come si è detto, per regola tecnica di sistema, l'eventuale chiave pubblica di B acquisita da un terzo sarebbe inutile per aprire il messaggio: al contrario dei sistemi simmetrici, dove l'acquisizione dell'unica chiave sarebbe fondamentale per la decifrazione del messaggio.

tabilità, e ad assicurare quindi la *funzione del non ripudio*[316], non potendo il mittente negare di avere inviato un messaggio ove lo stesso sia stato criptato con la sua chiave privata, come si desume dall'uso con successo di quella pubblica sul documento illegibile. In terzo luogo, nel caso della crittografia asimmetrica non si ha la necessità che le parti della comunicazione telematica si conoscano prima della stessa (al fine di scambiarsi l'unica chiave per procedere nelle operazioni di crittografia), problema insormontabile nelle varie applicazioni di *e-commerce* attuate tramite Internet, avendo a disposizione facilmente e costantemente nel tempo la chiave pubblica del soggetto che invia il messaggio[317].

La crittografia asimmetrica utilizzata in questo modo costituisce valido criterio di imputazione della paternità dei documenti informatici secondo diversi sistemi giuridici (si veda ad esempio il sistema adottato in Utah ed Illinois[318]), e sicuramente può essere considerato rientrante come minimo nella fattispecie delle firme elettroniche «deboli» previste dalla Direttiva 1999/93/CE e introdotte nel nostro Paese dal D Lgs. 23 gennaio 2002 n. 10[319]. Ma il legislatore italiano, per

[316] Questo almeno parzialmente, poiché infatti la possibilità del ripudio del messaggio in sé, o del suo testo, viene in realtà eliminata dalla tecnica della c.d. funzione di *hash*, come verrà spiegato oltre nel testo.

[317] Infine, la sicurezza circa l'integrità del documento in questo caso si otterrebbe non solo nei confronti dei terzi, ma anche fra le stesse parti della comunicazione, poiché esse non hanno la necessità di scambiarsi alcuna chiave segreta, ma ognuna rimane esclusivo detentore della propria: aspetto fondamentale nel caso in cui le comunicazioni elettroniche rivestano il carattere commerciale o debbano rivestire quello giuridico.

[318] Il riferimento è allo «*Utah Digital Signature Act*», entrato in vigore il 1 maggio 1995, e all'«*Illinois Electronic Commercial Security Act*», in vigore dal 14 agosto 1998, i cui testi sono reperibili su Internet all'indirizzo *http://ricerca.fst.it/osservatorioLegislativo/aspettiNormativi/normativePerStato/stato.asp.?Stato=55* (per la legge dello Utah) e *http://ricerca.fst.it/osservatorioLegislativo/aspettiNormativi/normativePerStato/stato.asp.?Stato=24* (per la legge dell'Illinois), entrambi consultati il 21 febbraio 2003.

[319] Anzi, quasi certamente un sistema di validazione dei documenti informatici basato sulla crittografia asimmetrica potrà rientrare tra le firme elettroniche avanzate o «forti». Al momento non sono ancora stati specificati in dettaglio i parametri tecnici sulla base dei quali classificare nell'ambito di una o dell'altra metodologia un determinato sistema di firma: né in tal senso è stata di aiuto la pubblicazione del regolamento previsto dall'art. 13, comma I, del D.Lgs. 10/2002 il D.P.R. 7 aprile 2003 n. 137. Gli unici riferimenti (anche se in maniera generica e non tecnica) possono allora riscontrarsi nel testo della direttiva, che nel suo Allegato III riporta i «Requisiti relativi ai dispositivi per la creazione di una firma sicura», e nella definizione

fare acquisire agli utenti la certezza relativa non solo alla provenienza del messaggio, ma anche alla sua integrità (cioè la sicurezza che il testo non abbia subito alterazioni dovute ad errori di trasmissione oppure ad interventi umani, e quindi non sia di fatto ripudiabile), oltre ad ottenere una maggiore sicurezza ed efficienza dell'intera tecnica[320], ha ideato un ulteriore sistema: la chiave privata, di regola, non viene applicata sull'intero messaggio, ma solo su di un estratto di esso (chiamato *hash code*, o «impronta»), estratto che viene automaticamente ricavato dal testo originale applicando allo stesso una funzione matematica detta di *hash*[321]. La criptazione dell'impronta del documento con la chiave privata del mittente costituisce la c.d *firma digitale*, ai sensi e per gli effetti del D.P.R. 28 dicembre 2000 n. 445 (e sue successive integrazioni e modifiche, in particolare quelle recentissime del D.P.R. 137/2003), che a pieno titolo può essere considerata una firma elettronica «*forte*» o avanzata che dir si voglia secondo quanto stabilito dal D.Lgs. 10/2002 e dal D.P.R. 137/2003. Volendo spiegare meglio quanto appena sinteticamente esposto, si procederà ora con il solito esempio. Dovendo A trasmettere a B un contratto con numerose pagine ed allegati, non usa immediatamente la sua chiave privata, ma prima esegue l'*hash*, ottenendo come risultato un documento di poche righe (l'*impronta*), al quale applica la sua chiave privata, criptando dunque solo questa: unisce, quindi, il risultato dell'operazione di criptazione dell'impronta (la firma digitale) al testo originario, che rimane leggibile in chiaro, e invia il tutto a B. Questi, dopo aver prelevato la chiave pubblica di A, la applica al testo ricevuto, ottiene l'*hash code*, ed allo stesso tempo acquisisce in questo modo la certezza della provenienza di quel messaggio proprio da A. Ese-

di «firma elettronica avanzata» contenuta nell'art. 2, lett. g) del D.Lgs. 10/2002 (ripreso nell'art. 1, lett dd del D.P.R. 137/2003. Ma su tali aspetti si veda oltre nel testo.

[320] Applicare infatti la chiave privata ad un documento molto lungo, da una parte implica la necessità di usare un sistema informatico potente per procedere nella criptazione, mentre dall'altra aumenta il rischio che si riesca a trovare il modo per decriptarlo. Si può quindi affermare che, anche nei sistemi asimmetrici, la sicurezza e l'efficienza del metodo è inversamente proporzionale alla lunghezza del testo da criptare.

[321] Questa può essere considerata uno specifico *software* che da un determinato testo di partenza di lunghezza variabile, dopo la sua applicazione, restituisce una stringa (l'impronta appunto, insieme di caratteri alfanumerici) di dimensioni fisse, che dipende direttamente dal documento originario: cambiando anche un solo carattere di questo, si modificherebbe il risultato della funzione, cioè l'impronta.

gue allora la funzione di *hash* sul testo originario, che aveva ricevuto in chiaro insieme alla firma digitale, ottiene nuovamente l'impronta, che va a questo punto a confrontare con quella appena decriptata: se il confronto è positivo, sarà allora sicuro che quello ricevuto è proprio il testo originario, e di conseguenza acquisirà la certezza della provenienza del documento da A e dell'impossibilità per questo di contestarlo (se le due impronte coincidono, vuol dire, infatti, che non è stato cambiato nemmeno un carattere del documento originario trasmesso dal mittente); se il confronto è invece negativo, avrà la certezza che il testo da lui ricevuto è in qualche parte diverso da quello originario inviatogli (o per un intervento di terzi, o perché lo stesso A ha modificato il messaggio – il suo testo in chiaro – dopo aver ricavato la firma digitale), e quindi, a seconda della fattispecie coinvolta, chiederà al mittente di ripetere l'intera operazione, oppure semplicemente ignorerà la comunicazione ricevuta[322].

Ecco, quindi, in cosa consiste la c.d. «firma digitale», *che non è poi una vera «firma», ma più correttamente un sistema di accertamento della titolarità di un documento elettronico basato su presunzioni giuridiche fondate su un sistema tecnico tendenzialmente sicuro*[323].

Se la tecnica appena esposta era, fino a poco tempo fa, l'unica tipologia di imputazione elettronica dei documenti informatici, occorre, invece, ora riportare le ulteriori fattispecie di sottoscrizione

[322] Altro più dettagliato esempio della procedura che implica la firma digitale si può leggere al § 45 del libro citato nella prefazione.

[323] Non perché assolutamente sicuro, e quindi teoricamente inviolabile (in realtà la tecnologia ha dimostrato che non esiste niente di veramente sicuro, ma solo correlato al tempo ed al costo per violarlo), o perché in ogni caso verrà rispettata la connessione soggetto titolare – chiave privata – firma digitale, ma perché il sistema prevede già i meccanismi per bilanciare la possibilità di mancata corrispondenza: il principio di *autoresponsabilità* per chi usa tale metodo (se smarrisco la chiave e non denuncio tempestivamente l'accaduto, sarò responsabile del suo uso), la possibilità di abbinare alla sicurezza tecnica delle chiavi una procedura (i soggetti certificatori, la vigilanza del Dipartimento dell'innovazione e la tecnologia, la possibilità di validazione temporale, etc.) che ha la possibilità di «reagire» adeguatamente ad eventuali problemi, le attribuzioni di responsabilità sui soggetti certificatori che svolgono l'importante compito di garantire la citata connessione, fin dal momento dell'individuazione dei loro requisiti (si veda l'art. 26, comma 1 del D.P.R. 445, così come modificato dall'art. 10 del D.P.R. 137/2003). Oltre infine al rilievo che, dipendendo certamente dai due parametri di costo e tempo per vincere le protezioni di sicurezza di un sistema, solo in alcuni limitati casi l'obiettivo bilancerebbe la spesa (sempreché si avessero comunque le capacità finanziarie per aumentare il livello tecnico delle protezioni).

informatica utilizzabili, introdotte dalle recenti novità legislative in materia, ed in genere le variazioni conseguenti. Infatti, in seguito al recepimento della Direttiva 1999/93/CE tramite il più volte richiamato D.Lgs. 10/2002, si affianca oggi alla firma digitale fin qui descritta, rigidamente disciplinata quale tecnica che unisce la crittografia asimmetrica con la funzione di *hash*, una firma elettronica c.d. «semplice» o «debole»: questa viene definita nella lett. *a*) dell'art. 1 del D.Lgs. 10/2002 come «l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica». La firma digitale, invece, viene conservata e diventa l'esempio principale (ma non unico) di firma elettronica «avanzata» o «forte»[324]: fattispecie che l'art. 1, lett. *g*), del Decreto definisce come «la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati».

La differenza tra le due riguarda soprattutto il grado di sicurezza relativa alla possibilità di accertare la provenienza e la genuinità del documento elettronico ad essa collegato (molto alta nel secondo caso, minore nel primo), e le conseguenze nel terreno delle prove processuali (che si analizzeranno nel prossimo paragrafo). Una maggiore specificazione del primo dei due sospetti appena indicati, in particolare i parametri tecnici che permettono di far rientrare un metodo di sottoscrizione informatica in una o nell'altra categoria di firma, al momento si può fare riferimento a quanto indicato nella Direttiva 1999/93/CE. Il suo Allegato III[325], infatti, dettato allo scopo di fis-

[324] Si tratta della cosiddetta «firma 5.1», dal paragrafo 1 dell'articolo 5 della direttiva 1999/93/CE, intitolato «Effetti giuridici delle firme elettroniche»: «1.Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura: a) posseggano, in relazione ai dati in forma elettronica, gli stessi i requisiti legali che una firma autografa possiede per i dati cartacei; b) siano ammesse come prova in giudizio».

[325] «1. I dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che: a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è ragionevolmente garantita la loro riservatezza; b) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro limiti ragionevoli di sicurezza, essere derivati e la firma è protetta da contraffazioni com-

sare i requisiti relativi ai dispositivi per la creazione di una firma sicura, e quindi disciplinando il mezzo tecnico per raggiungere il risultato di un sistema di validazione particolarmente efficace, permette di considerare «sicura» la firma elettronica che garantisce la riservatezza e la non alterabilità dei dati necessari alla creazione della stessa, che non sia esposta, entro limiti ragionevoli di sicurezza, a possibilità di contraffazione sulla base della tecnologia attualmente disponibile.

Considerando l'assoluta approssimazione con cui si è costretti a procedere al momento, si può pensare a questo punto di ipotizzare alcuni esempi tecnici da far rientrare in una o nell'altra categoria: così, si è detto (ed al momento può essere considerato l'unico dato certo) che la firma digitale del precedente sistema rientra sicuramente tra le firme elettroniche avanzate, così come vi si può far rientrare tutti i sistemi di sottoscrizione informatica basati sulla crittografia asimmetrica; sembrerebbero da considerare «deboli» le firme elettroniche basate invece su sistemi simmetrici, o su metodologie che affidano l'imputabilità a fattori che duplicano pedissequamente l'autografia (si pensi all'acquisizione mediante scanner della firma autografa da un supporto cartaceo, oppure direttamente con penna ottica e lavagna elettronica, «incollata» alla fine di un documento di testo). In attesa di un chiarimento sul punto, chiarimento necessario alla concreta operabilità del sistema (a meno di procedere solo sulla base delle pacifiche firme digitali, come infatti sta avvenendo per le applicazioni già in fase di attuazione: si pensi, ad esempio, al Registro telematico delle imprese), e prima di passare ad esaminare le conseguenze dell'applicazione di tale tecnologia al sistema di valutazione giuridica dell'attività di documentazione svolta attraverso l'uso dell'informatica e della telematica, ci si deve soffermare su un elemento fondamentale del sistema di sottoscrizione elettronica appena esposto.

215. *La firma digitale da un punto di vista strutturale: il 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, e diffusa il più possibile, per-

piute con l'impiego della tecnologia attualmente disponibile; c) i dati per la creazione della firma utilizzati nella generazione della stessa possono essere sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi. 2. I dispositivi per la creazione di una firma sicura non devono alterare i dati da firmare né impedire che tali dati siano presentati al firmatario prima dell'operazione di firma».

ché, come si è visto, costituisce elemento fondamentale per procedere nell'attività di verifica della provenienza del messaggio dal soggetto che ha utilizzato la corrispondente chiave privata. Il problema principale di tali sistemi è, però, quello di dare l'assoluta certezza, al soggetto che poi concretamente procede nell'attività di verifica, che la specifica chiave pubblica sia effettivamente del suo titolare: o, meglio, che il titolare di tale chiave sia chi dice di essere. Nei sistemi di firma digitale (detti P.K.I., cioè *Public Key Infrastructure*) tale problema relativo alla certezza della corrispondenza tra chiave pubblica e soggetto titolare cui essa appartiene viene in genere risolto attraverso la costruzione di specifici apparati di certificazione, 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 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*[326].

Questa figura di importanza fondamentale per qualsiasi *P.K.I.* solleva interessanti questioni, sia giuridiche che tecniche, relative al suo 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

[326] L'art. 22, comma I, del D.P.R. 445/2000 definiva, alle sue lettere *i*) ed *f*), sia il certificatore («*il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati*»), sia la procedura di certificazione («*il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni*»). Oggi, ai sensi dell'art. 8, lettere *b*) e *c*), del D.P.R. 137/2003, le sue definizioni appena indicate sono state abrogate, e si può fare riferimento, allo scopo di individuare la firma del «certificatore», al solo art. 1, lett. *u*), del D.P.R. 445/2000 ultima versione, cioè sempre dopo le modifiche introdotte dal D.P.R. 137 («il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime»).

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 riferiscono[327]; e 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 anche a livello legislativo.

Per quanto riguarda il nostro Paese, il legislatore con l'art. 27 del D.P.R. 445/2000, aveva disciplinato in maniera stringente i severi requisiti richiesti per svolgere l'attività economica di «certificatore», molto simili a quelli necessari all'esercizio dell'attività bancaria[328]. Fino all'emanazione del Dlgs 10/2002, e successivamente del D.P.R. 137/2003 che integra e coordina l'intero sistema, i soggetti che facevano richiesta di svolgere tale attività all'A.I.P.A. (l'autorità indipendente a cui all'epoca[329] era stato attribuito, dai primi interventi normativi in

[327] In cui quindi ogni soggetto oltre ad essere un utente del sistema, è anche certificatore della chiave pubblica degli altri: e questo a più livelli, sia per quello più semplice degli utilizzatori della crittografia asimmetrica (come avviene per il *P.K.I.* del più diffuso programma di crittografia asimmetrica, il *P.G.P.*, in cui la corrispondenza chiave-titolare è certificata 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), sia quindi nel caso proprio del livello delle autorità di certificazione.

[328] L'originaria versione dell'articolo 27 (*Certificazione delle chiavi*) disciplinava proprio nel suo terzo comma, alle lettere da *a)* a *d)*, i requisiti richiesti per i certificatori: «*a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati; b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche; c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 8, comma 2; d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale*». Oggi tale norma, come si vedrà oltre nel testo, è stata abrogata, e il sistema, ben più articolato e complesso rispetto alla sua versione iniziale, è disciplinato da diverse norme, che parzialmente ne richiamano il testo.

[329] Oggi, dopo diverse vicissitudini e numerose polemiche, l'A.I.P.A. ha ufficialmente cessato di esistere, almeno nella sua natura di autorità indipendente, ed in molti dei suoi compiti istituzionali, e si è trasformata in Centro Nazionale per l'Informatica nella Pubblica Amministrazione (non volendo perdere l'abitudine alle sigle, oggi quindi C.N.I.P.A.), costituito presso la Presidenza del Consiglio dei ministri. L'atto finale di questa «trasformazione» risale al luglio del 2003, e trova fondamento in una fonte certamente non destinata a disciplinare la materia indicata, in particolare il D.Lgs. 30 giugno 2003 n. 196 che istituisce il «Codice in materia di protezione di dati personali», il cui art. 176, infatti, dispone che il C.N.I.P.A. «opera presso la Presidenza del Consiglio dei Ministri per l'attuazione delle politiche del Ministro per l'Innovazione e le Tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio». Sul punto si veda, oltre ai numerosi articoli di cronaca pubblicati nei maggiori quotidiani nazionali sull'argomento, F. Loppini, *Addio AIPA, benvenuto CNIPA*, su Internet nel sito *Jei*, all'indirizzo *http://www.jei.it/infogiuridica/notizia.php?ID_articoli=245* consultato il 10 ottobre 2003.

materia, il compito di gestire l'infrastruttura del sistema di firma digitale italiano, in pratica il certificatore dei Certificatori), in caso risultassero dotati degli indicati requisiti, venivano iscritti in un elenco pubblico gestito da tale Autorità: essa effettuava poi uno stringente controllo circa la sussistenza nel tempo delle caratteristiche richieste dalla legge[330].

Il più volte ricordato Dlgs 23 gennaio 2002 n. 10, modificando radicalmente la struttura del sistema di certificazione delle firme digitali, liberalizza (secondo gli intendimenti della Direttiva comunitaria 1999/93/CE) certamente il settore, ma in una maniera un po' troppo complicata e a tratti oscura. Innanzitutto viene sostituito l'organo che vigila sui Certificatori, non più l'Autorità per l'Informatica nella Pubblica Amministrazione, ma il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri[331];

[330] Fino ad oggi, e prima dell'intervento del legislatore in adempimento della direttiva 1999/93/CE, i certificatori italiani ufficialmente riconosciuti erano 14 società (a cui si era da ultimo aggiunto anche il Consiglio Nazionale del Notariato), il cui elenco era consultabile sul sito dell'A.I.P.A. all'indirizzo *http://www.aipa.it/attivita[2/certifica[17/* mentre oggi è possibile reperirlo nel nuovo sito del C.N.I.P.A. all'indirizzo Internet *http://www.cnipa.gov.it/site/it-IT/Le_Attivit%c3%a0/Elenco_certificatori/* visitato il 10 ottobre 2003: in tale materia è intervenuto sostanzialmente, come si è detto e come si vedrà oltre nel testo, il D.Lgs 10/2002 e più recentemente il D.P.R. 137/2003 (oltre alle trasformazioni tipiche conseguenti allo svolgimento di attività economiche, che hanno portato 3 società a cessare la loro attività di certificatore, ed altre a subentrare, fino a raggiungere all'ottobre 2003 il numero di 13).

[331] L'A.I.P.A. veniva ad essere, in materia di firme elettroniche, uno degli organismi a cui l'indicato Dipartimento *poteva* rivolgersi per svolgere le proprie funzioni di vigilanza e controllo (si vedano a tale proposito le disposizioni degli artt. 3, comma 2, e 4, comma 2, del D.Lgs 10/2002): scelta di sistema che, portando una netta diminuzione dell'importanza delle funzioni e dei compiti dell'Autorità (meramente consultive, tra l'altro a livello facoltativo), suscitava diverse perplessità, e che

poi, l'attività di controllo viene notevolmente ridimensionata, in diretto collegamento alla volontà del soggetto che vuole svolgere l'attività di certificazione delle firme elettroniche, e che viene previsto si possa proporre su diversi livelli.

Così tale soggetto, se vuole semplicemente prestare servizi di certificazione di «base» (cioè con un relativo livello di qualità e sicurezza) o altri servizi connessi, non avrà bisogno di alcun tipo di autorizzazione preventiva e lo potrà fare liberamente. Nel caso, invece, che il certificatore voglia rilasciare attestati con un rilevante livello di qualità e sicurezza, dovrà semplicemente dare avviso dell'inizio dell'attività al citato Dipartimento, anche in via telematica: in questo caso, ipotesi dei certificatori c.d. «*qualificati*», il controllo dello stesso sarà solo successivo (chiamato, nella relazione illustrativa del D.Lgs. 10, «supervisione»), d'ufficio o dietro segnalazione motivata. Il Decreto prevede anche l'ipotesi dei certificatori c.d. «*accreditati*»: sono quelli con i requisiti di qualità e sicurezza più elevati, che hanno chiesto di essere riconosciuti tali e che, avendo soddisfatto i requisiti richiesti per il loro accreditamento, sono stati inseriti nell'apposito elenco pubblico tenuto dallo stesso Dipartimento per l'innovazione e le tecnologie (tra questi rientreranno automaticamente i 15 che erano stati riconosciuti dall'A.I.P.A., come viene esplicitamente disposto dall'art. 11, comma 2, del D.Lgs. 10/2002, oggi ridotti a 13). Chiaramente il controllo su di essi sarà più «rigido», questa volta non solo successivo, ma anche preventivo.

Nel silenzio della norma, volendo creare una corrispondenza tra il metodo tecnico utilizzabile per validare un documento elettronico e il soggetto che attesta la corrispondenza chiave-titolare, si può supporre che le firme elettroniche «forti» potranno solo essere certificate dal secondo e terzo tipo di certificatori (qualificati e accreditati), mentre quelle «deboli» anche dai semplici certificatori del primo tipo.

Sul sistema appena indicato ha poi ulteriormente influito il D.P.R. 7 aprile 2003 n. 137, il «Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del

aveva provocato un vivace dibattito e forti prese di posizione da parte dei componenti della stessa Autorità (si pensi alle dimissioni del presidente Zuliani presentate il 1 febbraio 2002, notizia riportata il giorno dopo dai principali quotidiani). Oggi, soppressa definitivamente l'A.I.P.A., e trasformata nel «Centro Nazionale per l'Informatica nella Pubblica Amministrazione» (C.N.I.P.A.), le perplessità sono rimaste immutate, nonostante le diverse assicurazioni prestate circa il costante mantenimento della sua autonomia da parte del Governo.

decreto legislativo 23 gennaio 2002, n. 10», che avrebbe dovuto rappresentare la norma di «chiusura» del sistema italiano di validazione giuridica della documentazione elettronica, definendo differenti aspetti dello stesso lasciati in forma generica dai diversi interventi del Legislatore in materia, chiarendo i numerosi dubbi sollevati dalle precedenti fonti e dalla loro applicazione, coordinando le diverse disposizioni delle stesse. Purtroppo le finalità indicate non sono state raggiunte, se non parzialmente, mentre un testo spesso oscuro ed a tratti incoerente ha portato alla nascita di ulteriori difficoltà di interpretazione e quindi di applicazione pratica.

Per quello che interessa l'argomento del presente paragrafo, la disciplina della figura del certificatore, il D.P.R. 137/2003 ha modificato il testo del D.P.R. 445/2000 in materia di requisiti degli stessi. Così, i parametri che devono essere rispettati per poter rientrare nella categoria dei certificatori c.d. «*qualificati*» sono indicati nell'art. 27 nuova versione[332], mentre per la categoria dei certificatori c.d. «*accreditati*» il riferimento è all'art. 28[333].

[332] Art. 27 D.P.R. 445/2000 nel testo ora vigente «*1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26. 2. I certificatori di cui al comma 1 devono inoltre: a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione; b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2; c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate; d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10; e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi. 3. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente testo unico, ai sensi dell'articolo 4, comma 1, del decreto legislativo 23 gennaio 2002, n. 10* (...)».

[333] Art. 28 D.P.R. 445/2000 nel testo ora vigente «(...) *2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27 ed allegare alla domanda il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei cer-*

Vengono infine individuate precise ipotesi di responsabilità dei certificatori. L'art. 7, in particolare, prevede infatti, attraverso anche una modifica testuale del DPR 445/2000 (viene infatti aggiunto l'art. 28-*bis* proprio a disciplina di questo aspetto), che il certificatore sia responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento sull'esattezza e completezza delle informazioni contenute nel certificato, e dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato.

Individuata la tecnologia utilizzata per dare certezza giuridica agli atti documentali gestiti attraverso l'uso dell'informatica e della telematica, e descritto il soggetto principale a livello di struttura del sistema di sottoscrizione elettronico, il c.d. Certificatore, si procederà ora ad esaminare gli aspetti relativi alla natura ed al valore giuridico del documento informatico corredato dalla firma elettronica o da quella digitale.

216. *Il valore giuridico del documento informatico nel sistema italiano di firma digitale o elettronica.* – Il complesso sistema appena descritto, volto a riconoscere un fondamento giuridico alla documentazione formata, gestita e comunicata attraverso elaboratore elettronico, è stato adottato nel nostro Paese attraverso una peculiare metodologia normativa: peculiarità motivata dalla non semplice struttura tecnica del sistema, dalla realtà su cui è destinata ad influire (radicate procedure tradizionali, una diffusa situazione di mancata cultura delle nuove tecnologie, la burocratica gestione della Pubblica Amministrazione) e probabilmente dalla volontà di consentire un adeguamento progressivo, e per quanto possibile «indolore», degli apparati di documentazione.

Così, si è giunti alla radicale innovazione del quadro normativo

tificati nonché l'impegno al rispetto delle regole di tecniche. 3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre: a) avere natura giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385; b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti il collegio sindacale, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 citato del decreto legislativo 1° settembre 1993, n. 385 (...)».

di riferimento e all'introduzione della disciplina giuridica del documento informatico (con la tipizzazione di un sistema di firma digitale quale criterio legale di imputazione del documento formato mediante il computer) attraverso un procedimento complesso, ed ancora in fase di realizzazione, in cinque diversi momenti:

- *innanzitutto* con l'art. 15, comma II, della legge 59/1997 che stabilisce 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. 513/1997 (appunto il Regolamento richiamato), che pone quindi una complessa disciplina in 22 articoli, sottoposta a numerose critiche e ad emanazione travagliata, e che procede (art. 3, comma I, del D.P.R. 513) ad un ulteriore rinvio per la fissazione delle regole tecniche idonee a renderne effettiva l'applicazione[334];
- *poi*, con il D.P.C.M. 8 febbraio 1999 finalizzato proprio a stabilire le specifiche tecniche del D.P.R. 513/1997;
- *ancora*, con il D.P.R. 445/2000, il «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa», fonte che nasce dall'esigenza di raccogliere in un unico provvedimento quanto prodotto, in tema di semplificazione dell'attività amministrativa, da tre anni e mezzo di attività legislativa, e che quindi abroga recependo integral-

[334] In realtà i rinvii sono diversi, non solo quello dell'art. 3: si devono infatti ricordare anche quello effettuato dall'art. 4, comma II, ad un futuro decreto del Ministero delle Finanze per la disciplina degli aspetti fiscali della documentazione elettronica, e quelli dell'art. 18, comma III, e 20, comma I, a regole e norme tecniche da emanarsi ad opera dell'Autorità per l'Informatica nella P.A. (le prime in materia di formazione e conservazione dei documenti informatici, le seconde per lo sviluppo dei sistemi informativi delle P.A.). Altra produzione che si attende è, da una parte, quella che andrà a sostituire le norme tecniche dettate con il D.P.C.M. 8 febbraio 1999 (in netto ritardo rispetto al termine biennale stabilito nell'art. 8, comma 3, del D.P.R. 445/2000), e, dall'altra, quella prevista dall'art. 13, comma 1, del D.Lgs 10/2002, che tra l'altro ha il fondamentale compito di effettuare un coordinamento tra le varie fonti indicate.

mente il D.P.R. 513/1997 (diventando in questo modo il testo di riferimento in materia di firme elettroniche e digitali);
- *recentemente*, con il Dlgs 10/2002, che recepisce nel nostro ordinamento la Direttiva 1999/93/CE, introducendo rilevanti novità nell'intero sistema di validazione giuridica dei documenti elettronici, come più volte rilevato nelle pagine precedenti.
- *infine*[335], con il D.P.R. 137/2003 che, come si è detto, avrebbe dovuto rappresentare la norma di «chiusura» del sistema, coordinando e chiarendo le varie fonti appena indicate, mentre invece il suo testo spesso oscuro ed a tratti incoerente ha portato alla nascita di ulteriori difficoltà di interpretazione e quindi di applicazione pratica, facendo quasi auspicare un ennesimo intervento legislativo volto, in maniera definitiva, a razionalizzare effettivamente, ed a chiarire, l'intero sistema italiano delle firme elettroniche nei suoi differenti aspetti giuridici, tecnici ed applicativi.

Con la realizzazione di tale processo, ed anche a prescindere dalla sua attuazione concreta (comunque oramai già avviata e di prossimo completamento), l'Italia è stato uno dei primi Paesi al mondo ad aver compiuto un importante passo per recepire l'innovazione tecnologica nel proprio sistema economico-giuridico[336].

Così, la firma digitale, cioè quella realizzata attraverso l'uso della crittografia a chiave pubblica certificata corredata dalla già citata fun-

[335] Sono state elencate le principali fonti in materia di firma digitale, alle quali deve essere riferita anche un'altra produzione secondaria costituita da delibere e circolari A.I.P.A., ora da quelle del C.N.I.P.A., poi da decreti e regolamenti di diverse altre autorità, volte in genere a disciplinare aspetti tecnico-organizzativi del sistema, e di cui quindi non ci occuperemo in questa sede.

[336] E questo può forse essere considerato il principale risultato positivo della disciplina esaminata nel presente scritto: infatti, allo stesso modo in cui l'emanazione della l. 31 dicembre 1996 n. 675, in materia di tutela dei dati personali, ha avuto come conseguenza la nascita e la diffusione di una «cultura della riservatezza», cioè di una nuova e particolare attenzione relativa alla protezione della sfera più intima dell'individuo, così l'articolato sistema della firma digitale potrebbe costituire un grosso stimolo alla diffusione della «cultura della tecnologia». E, in un momento storico come quello che stiamo vivendo, in cui ogni giorno vengono annunciate importanti novità nei più diversi settori, novità strettamente dipendenti dalle applicazioni dell'informatica e della telematica, se al semplice «uso» della tecnologia si sostituisse un «uso consapevole» della stessa, si potrebbe maggiormente controllare il rivoluzionario avvento dell'innovazione tecnologica, evitando così le sue implicazioni negative ed aumentando invece quelle positive.

zione di *hash*, costituisce oggi in Italia il criterio legale di imputazione del documento redatto mediante il computer. È cioè lo strumento mediante il quale l'ordinamento giuridico riesce ad attribuire il valore di piena prova alla documentazione prodotta, gestita e trasmessa attraverso l'utilizzo dell'elaboratore elettronico, equiparandola alla tradizionale scrittura privata, ma prescindendo dalla necessità della sua resa cartacea, della sua stampa. Questo risultato è stato ottenuto senza necessità di modificare le leggi esistenti, ma semplicemente ampliando la portata dei concetti giuridici tradizionali (ad esempio «documento» non è più considerato il solo foglio di carta, ma anche l'insieme di *byte* memorizzati nei circuiti del computer che magari rappresentano la versione digitale di una fotografia o di un suono), operazione compiuta sulla base di una tecnologia sicura, quella della firma digitale appunto, e che ha reso possibili e valide diverse attività: non solo la conclusione di contratti in forma elettronica[337], ma l'invio in genere di documenti usando la posta elettronica[338], la richiesta di certificati alla P.A., le operazioni di archiviazione ottica della documentazione amministrativa, ...

Il documento informatico con firma digitale certificata viene, quindi, considerato dal legislatore (e conseguentemente la stessa valenza dovrà essere data da tutti coloro che ne vengono in contatto)

[337] Magari su Internet, grazie all'art. 11 del DPR 445/2000 che dispone che i «contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma elettronica qualificata» sono validi e rilevanti a tutti gli effetti di legge. Così, ad esempio, se sorgesse una contestazione relativa alla trattativa svolta mediante *e-mail* con firma digitale per concludere un contratto, una qualsiasi delle parti potrebbe presentare al giudice che dovrà pronunciarsi sulla controversia il documento contestato in forma digitale (magari inviandolo ancora attraverso la posta elettronica alla cancelleria del tribunale, quando verrà realizzato il c.d. processo telematico, oppure consegnandolo alla stessa in un *floppy disk* che lo contiene).

[338] In base all'art. 14 del DPR 445 si può considerare infatti inviato e pervenuto al destinatario il documento informatico trasmesso all'indirizzo dello stesso per via telematica: si pensi a tale proposito alle comunicazioni tra imprese e Camere di commercio, che ai sensi dell'art. 31, comma 2, della l. 340/2000 avverranno obbligatoriamente per via telematica, come si vedrà oltre. In questa sede si deve sottolineare l'importanza dell'art. 14 citato che, insieme anche all'art. 22, comma 1, lett. *h*), dell'indicato decreto (norma che introduce il concetto di «indirizzo elettronico», quale «*identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici*»), ha il grande merito di far entrare nel nostro ordinamento con piena efficacia i sistemi di posta elettronica (e correlativamente Internet) e la comunicazione attraverso essi, prassi sempre più consolidata anche nel mondo degli affari per evitare le lentezze, e in genere i problemi della tradizionale posta cartacea.

come documento *scritto*, ed in particolare come se fosse un documento cartaceo firmato a mano dal soggetto che lo ha prodotto. Invece i documenti elettronici senza la firma digitale o quella elettronica previste dalla legge possono liberamente essere utilizzati, ma, in caso di contestazione, il giudice eventualmente investito della questione gli attribuirà, come si vedrà oltre, il valore probatorio delle riproduzioni meccaniche stabilito nell'art. 2712 cod. civ.

Sul nuovo valore probatorio dei documenti prodotti attraverso l'uso dell'elaboratore elettronico era chiarissimo il disposto dell'art. 23 del D.P.R. 445/2000, 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 prevedeva: «*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*». Previsione oggi modificata slla base dell'art. 9 del D.P.R. 137/2003 (che ne ha reso, perseguendo il dichiarato scopo dell'intero decreto – quello di semplificazione e coordinamento –, molto più oscuro e meno efficace il testo), ma il cui testo originale permette ancora di rilevare, in tutta la sua importanza, la portata innovativa della disciplina legislativa sulla firma digitale: una rivoluzione nella valutazione giuridica dell'attività di documentazione attraverso elaboratore elettronico, svolta ampliando come già detto la portata di categorie concettuali tradizionali, come quella di documento o di sottoscrizione.

La natura giuridica ed il valore probatorio delle «cose rappresentative di un fatto» quando sono prodotte attraverso un sistema di elaborazione dati viene, invece, stabilita nell'art. 10 del D.P.R. 445/2000: norma (intitolata proprio «Forma ed efficacia del documento informatico») che ha raccolto in un'unica disposizione i due articoli originari del D.P.R. 513/1997 in materia, e che è stata recentemente sostituita integralmente dall'art. 6 del D.Lgs. 10/2002, per renderla maggiormente coerente a quanto disposto dalla Direttiva comunitaria in materia di firme elettroniche (in particolare del suo art. 5), con una versione testuale maggiormente corretta e comprensibile rispetto alla precedente. Risultano essere di interesse i primi tre commi.

Così, secondo il primo comma, è il documento informatico in sé, a prescindere da qualsiasi forma di attribuzione della sua paternità (e quindi nel caso non si utilizzi alcuna firma elettronica), ad assumere il valore probatorio della riproduzione meccanica disciplinata dall'art. 2712 del codice civile: ha quindi il valore di piena prova, se

non viene disconosciuto da colui contro il quale viene prodotto, dei fatti o delle cose in essa rappresentati[339].

Il secondo comma contempla l'ipotesi del documento informatico a cui è stata apposta il nuovo tipo di sottoscrizione attuata attraverso l'uso dell'elaboratore elettronico, quella creata dalla Direttiva 1999/93/CE ed introdotta nel nostro ordinamento dal D.Lgs. 10/2002: la c.d. firma elettronica «semplice», o «debole» (anche se il testo della norma riporta la sola dizione «firma elettronica»), che si ricorda viene definita come l'«insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica» (art. 1, lett. *a*), e che risulta dotata di un relativo grado di sicurezza circa la possibilità di accertare la provenienza e la genuinità del documento elettronico ad essa collegato. Si tratta di un nuovo tipo di sottoscrizione che si è detto essere stato introdotto per consentire di effettuare imputazioni di paternità di documenti informatici senza le formalità, le complicazioni ed i costi delle vere e proprie firme digitali[340]. Il legislatore in particolare stabilisce che tali documenti *soddisfano il requisito legale della forma scritta*, ripetendo così, ma questa volta specificandola meglio, una delle più importanti disposizioni dell'originario D.P.R. 513/1997[341]. Fino a quel momento, infatti, alla conclusione circa la

[339] Ed in questo modo viene superata la difficoltà interpretativa delle prime versioni della disciplina probatoria dei documenti informatici con firma digitale.

[340] Si tenga presente che il processo relativo all'applicazione di una firma digitale è sicuramente gravoso dal punto di vista economico (si pensi, a parte il costo del sistema informatico, all'onere relativo alla certificazione, ed all'eventuale deposito, della chiave pubblica).

[341] Il riferimento è all'art. 4 del D.P.R. 513, rispetto al quale, in particolare rispetto al collegamento tra riconoscimento di natura di documento scritto e necessità per il documento informatico di essere munito dei requisiti richiesti dallo stesso D.P.R. (che presumibilmente erano la sola apposizione di firma digitale), si sollevavano diverse perplessità. Ci si chiedeva, infatti, quale fosse la natura giuridica dei documenti informatici non muniti degli indicati requisiti, e quindi senza firma digitale, giungendo a negare loro la natura di documenti scritti. La gravità di una conclusione in tal senso, a parte i rilievi relativi addirittura ad un arretramento rispetto alle posizioni sull'argomento oramai consolidate in dottrina e giurisprudenza e in alcune fonti normative precedenti al D.P.R. 513 (di cui si è parlato nelle pagine precedenti), si coglieva nel considerare il sistema nel suo insieme: a fronte della complessità del procedimento relativo all'uso delle tecniche di firma digitale, si riteneva infatti oltremodo inopportuno diminuire l'importanza delle attività alternative di documentazione elettronica, in particolare tenendo presente i presumibili costi e le evidenti complicazioni del sistema delle firme digitali.

natura di «documento scritto» anche nel caso di documenti prodotti attraverso elaboratore elettronico e conservati in forma magnetica nelle sue memorie circuitali, giungeva solo una parte della dottrina, in particolare quella maggiormente incline all'uso dei nuovi strumenti[342]. Il secondo comma della nuova versione dell'art. 10, a tale proposito, prevede anche che il documento informatico con firma elettronica «debole» soddisfi l'obbligo previsto dagli artt. 2214 e seguenti del codice civile (quello cioè relativo alla tenuta delle scrittura contabili): previsione nei confronti della quale una parte della dottrina specializzata ha assunto una posizione nettamente critica, anche se in maniera non totalmente comprensibile, soprattutto se si collegano le vivaci polemiche agli sforzi che storicamente sono stati compiuti per permettere il riconoscimento della natura di documento scritto al documento informatico *tout court*, a prescindere da alcuna sottoscrizione elettronica.

Con riferimento, infine, al vero e proprio valore probatorio del documento con firma elettronica semplice, la norma dispone che esso potrà essere liberamente valutato dal giudice interessato di un'eventuale controversia sullo stesso: nella valutazione chiaramente si terrà conto delle caratteristiche oggettive di qualità e sicurezza dello stesso.

Il terzo comma dell'art. 10 completa il nuovo sistema di validazione giuridica della documentazione prodotta attraverso l'uso di un computer, contemplando il valore probatorio della firma elettronica c.d. «avanzata» o «forte»: fattispecie che il Decreto (art. 1, lett. *g*) definisce come «la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, *creata con mezzi sui quali il firmatario può conservare un controllo esclusivo* e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati», e che risulta dotata di un alto grado di sicurezza circa la possibilità di accertare la provenienza e la genuinità del documento elettronico ad essa collegato.

Esplicito nel comma in esame è inoltre il riferimento alla firma digitale, che viene comunque conservata, ed anzi diventa l'esempio principale (ma non unico) del nuovo genere di sottoscrizione.

Per quanto riguarda la natura giuridica ed il valore probatorio del documento elettronico munito di firma elettronica avanzata, il

[342] In particolare Giannantonio, Borruso, nelle loro opere più volte citate, su cui si veda quanto detto in precedenza.

terzo comma stabilisce che il documento prodotto attraverso l'uso di un computer debba essere considerato non soltanto certamente *scritto*, ma con un valore probatorio maggiore di quello della scrittura privata, addirittura come se fosse *riconosciuta* ai sensi degli artt. 2702 e 2703 del codice civile (sicché il firmatario non potrà disconoscere la propria sottoscrizione elettronica se non con il complesso procedimento della querela di falso).

Anche questa disposizione, come quella relativa al valore di «forma scritta» attribuito dal secondo comma dell'art. 10 al documento informatico munito di firma elettronica semplice, ha suscitato numerose critiche da parte di alcuni esperti del settore: in tale caso le polemiche riguardavano l'equiparazione di fatto, attuata dalla nuova versione del terzo comma, della «scrittura privata elettronica» a quella legalmente riconosciuta. In particolare venivano sollevate notevoli perplessità circa l'opportunità di richiedere l'attivazione della complessa procedura della querela di falso al fine di contestare la veridicità della documentazione informatica a cui è stata apposta una firma digitale, invece della più semplice possibilità del disconoscimento della scrittura privata riservata alla realtà della documentazione cartacea tradizionale[343]; oltre a rilevare l'apparente incongruenza tra la nuova versione della norma e la conferma della figura della firma digitale riconosciuta disciplinata dall'art. 24 del D.P.R. 445/2000[344].

Al di là comunque delle varie difficoltà interpretative sollevate dal testo della norma, e dalla peculiare «storia normativa» del sistema italiano di validazione giuridica dell'attività di documentazione svolta attraverso l'informatica e la telematica, l'innegabile utilità ed efficienza dei nuovi strumenti ha portato ad un loro crescente utilizzo, ed alla

[343] Manifestazione concreta del più generale problema interpretativo che era stato sollevato relativamente al valore giuridico del documento elettronico firmato digitalmente, in cui si registrava il contrasto tra la posizione di coloro che gli attribuivano il valore della scrittura privata in sé riconosciuta, e coloro che invece applicavano la medesima struttura del sistema codicistico tradizionale (a tale proposito da ultimo si veda F. Tommasi, *Firma digitale, contratti sicuri*, in *Fisco e diritto delle nuove tecnologie, Le guide operative di Guida al Diritto*, Sole 24 Ore ed., 2002, pp. 61-69). A tale proposito, non volendo entrare in maniera approfondita in tali contrasti dottrinari, in sede di commento della norma ci si limita ad osservare che la soluzione della diatriba deve essere cercata comunque tenendo presente la realtà tecnologica della documentazione informatica, ed evitando quindi inutili ed impossibili duplicazioni di discipline rispetto alla realtà cartacea.

[344] A tale proposito si veda quanto si dirà nelle prossime pagine relativamente all'argomento.

nascita di sempre più interessanti applicazioni[345]: si pensi in particolare alla trasmissione telematica delle dichiarazioni fiscali e previdenziali, già utilizzata fin dal gennaio del 1999, e via via estesa a settori sempre più vasti di utenti (inizialmente è stata attuata solo per i commercialisti ed i consulenti del lavoro, poi sono stati aggiunti i Centri di Assistenza Fiscale e altri liberi professionisti, infine anche i semplici contribuenti); si considerino, poi, le possibilità offerte ai notai di registrare gli atti di compravendita direttamente *on line*, ai professionisti abilitati ad operare nel settore di trasmettere per via telematica le denunce al Catasto dei fabbricati ed a quello dei terreni, nonché le prime concrete attuazioni, sia pure a livello sperimentale, del decreto del Ministero della Giustizia 13 febbraio 2001 n. 123 sul c.d. processo telematico[346]; ci si riferisce, infine, all'obbligo, stabilito dall'art. 31, comma 2, della l. 24 novembre 2000 n. 340, di presentare al Registro Imprese le denunce e gli atti che le accompagnano unicamente in via telematica e sottoscritte dal legale rappresentante della società con firma digitale, obbligo che è già entrato in vigore dal 9 dicembre 2002 (anche se con possibilità alternative fino al 30 giugno 2003[347]).

Di tale utilizzo la categoria che maggiormente si è fatta portatrice è quella dei notai, come si vedrà diffusamente nel prossimo paragrafo.

[345] Anche se poi, proprio la complessa procedura utilizzata per il recepimento dell'indicata tecnica nell'ordinamento giuridico del nostro Paese, oltre alle difficoltà culturali generalmente sollevate dalla tecnologia, ha portato a forti ritardi proprio nella sua applicazione generalizzata.

[346] «Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo innanzi alle sezioni giurisdizionali della Corte dei conti», pubblicato nella G.U. 17 aprile 2001 n. 89.

[347] Così in seguito alla modifica stabilita dall'art. 3, comma 13, della l. 448/2001 (legge finanziaria per il 2002, che ha prorogato il termine iniziale previsto nella l. 340/2000 di un anno: quindi complessivamente l'obbligo della comunicazione telematica scattava decorsi due anni dal 9 dicembre 2000), e recentemente dalla Circolare del Ministero delle attività produttive n. 2553 del 29 novembre 2002 e dall'art. 13-*ter* della l. 27 dicembre 2002, n. 284 (la legge che converte il decreto-legge 236/2002 in materia di termini legislativi in scadenza). Con riferimento all'automazione del sistema di pubblicità legale delle imprese si veda G. Ciacci, *Atti societari e firme elettroniche: il Registro delle imprese telematico*, e G. Ciacci, *Avvio* soft *per il Registro delle imprese*, in *Diritto e Pratica delle Società*, Il Sole 24 Ore Ed., rispettivamente Marzo 2002, n. 6, pp. 21-26, e febbraio 2003, n. 2, pp. 28-32.

217. *Il notariato informatico.* – Occorre subito evidenziare alcuni aspetti peculiari della figura del notaio rispetto alle nuove tecnologie, ed in particolare rispetto al sistema della firma digitale e di quella elettronica quale sistema per dare valore giuridico al documento informatico: da una parte perché la posizione del notariato nei confronti dell'informatica è sempre stata molto aperta[348], totalmente diversa rispetto a quella di altri operatori del diritto, come ad esempio la classe forense; dall'altra perché è lo stesso DPR 445/2000 a prendere in considerazione la figura del notaio nel disciplinare la firma digitale e quella elettronica, stabilendo per lui alcune funzioni specifiche anche nel nuovo sistema.

Dal primo punto di vista, l'approccio nei confronti delle nuove tecnologie, è già stata rilevata l'apertura dei notai 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[349]; ed in tale ottica ha visto la luce da una parte la società Notartel, costituita nel 1997 e dedicata allo sviluppo di servizi informatici telematici per i notai italiani, che ha quindi la gestione operativa di tutti i progetti coinvolgenti le nuove tecnologie del Consiglio Nazionale del Notariato, e, dall'altra, la Rete Unitaria del Notariato che, dopo soli pochi mesi dalla sua attivazione collegava circa 1.000 notai su 4.500[350].

[348] Anche se poi, nonostante tale approccio molto aperto, si deve registrare anche per tale categoria una lentezza generalizzata nel completamento delle procedure di automazione, oltre al non così immediato coinvolgimento dell'utente finale, il singolo notaio.

[349] «Il notaio è abituato da sempre a seguire l'evoluzione della società, sia sotto il profilo giuridico, che sotto quello tecnologico. Sotto il profilo giuridico, la modifica costante e a tratti impetuosa della legislazione impone al notaio una capacità di adattamento immediato, ancor prima di quanto debbano fare le altre categorie degli operatori giuridici, gli avvocati, i giudici, che normalmente sono chiamati ad applicare la norma dopo un congruo periodo di riflessione e di elaborazione. Sotto il profilo tecnologico, il fatto che la professione notarile sia a contatto con il mondo dell'impresa, ha stimolato un adattamento sufficientemente rapido alle evoluzioni. In questo quadro, tutto ciò che dà certezza e maggiore efficienza non può che vederci favorevoli e pertanto siamo convinti che lo sviluppo della telematica porterà dei vantaggi sia alla nostra categoria professionale, sia al cittadino, soprattutto se anche la Pubblica Amministrazione, come sta facendo, si adeguerà» (così P. Piccoli, *Una intranet dei notai per autenticare gli atti digitali*, in *http://www.ingenium.it/23tavrot.html* consultato il 21 febbraio 2003).

[350] Tale rete persegue fondamentalmente due obiettivi: realizzare un supporto

Dal secondo punto di vista, e cioè la considerazione della figura del notaio da parte del D.P.R. 445, si devono ricordare: l'art. 20, comma 3, 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; «*presso un notaio o altro pubblico depositario autorizzato*»; l'art. 24, in materia di firme digitali autenticate[351], ed infine l'art. 13 in tema di libri e scritture formati e conservati su supporti informatici con firma digitale[352]. Vediamo ora in maniera particolareggiata i due aspetti.

218. *Le applicazioni della firma digitale ed il notaio.* – Come si è detto, il sistema della firma digitale e di quella elettronica crea, quindi, per il notaio una nuova serie di attività[353], oltre a permettere di dare fondamento giuridico a quelle che già in passato venivano gestite attraverso l'uso dell'elaboratore elettronico. Per quanto riguarda le prime, in aggiunta a quelle attivate grazie alla Rete Unitaria del Notariato (e, dunque, quelle proprie di Internet e dei servizi da tale rete resi possibili, da una parte, e quelle informative più tipicamente

comunicativo evoluto, in grado di gestire documenti complessi, e di mettere in contatto i notai tra di loro, e questi con il Consiglio Nazionale del Notariato, la Pubblica Amministrazione ed in genere il mondo esterno; rendere disponibile un sistema telematico con elevati livelli di affidabilità e sicurezza, sia ai fini comunicativi appena esposti, sia per la gestione di informazioni di interesse comune alla categoria e di applicazioni di diversa complessità e tipologia. Per avere notizie aggiornate su tale Rete si può consultare il sito web del Consiglio, all'indirizzo *http://www.notariato.it*.

[351] Relativamente a tale articolo, che ha suscitato diverse polemiche tra gli studiosi della materia, ma anche per gli altri appena citati, si veda quanto riportato, in sede di commento al D.P.R. 445/2000, da G. Ciacci, *La firma digitale*, cit., pp. 107-192.

[352] Nel testo del D.P.R. 445/2000 prima delle modifiche recentemente apportate dal D.P.R. 137/2003 vi era anche un'altra norma che si riferiva al notaio: l'art. 26, infatti, disponeva in materia di deposito, in forma segreta, della chiave privata di un soggetto, che poteva essere effettuato «presso un notaio o altro pubblico depositario autorizzato». Tale previsione non è stato poi ripreso in alcuna parte della nuova formulazione del D.P.R. 445.

[353] 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 R.G. Barresi, *Aspetti comparatistici del notariato fra Italia e Inghilterra*, in *Vita notarile*, ottobre 1998, e M. Miccoli, *Cybernotary*, in *Notariato*, 1996, p. 107).

collegate alla professione notarile, come ad esempio la possibilità di effettuare a distanza le visure catastali, quelle camerali, quelle ipotecarie in conservatoria e quelle automobilistiche al P.R.A., dall'altra), si possono poi segnalare le applicazioni collegate al modello unico informatico e quelle relative all'invio *on line* degli atti societari ed al Registro telematico delle imprese.

Con riferimento nella specie al modello unico informatico, cioè quella particolare procedura che permette ai notai di adempiere per via telematica gli obblighi inerenti la registrazione, trascrizione e voltura degli atti relativi a diritti sugli immobili[354], lo scopo che ha portato in questo caso a dare un riconoscimento normativo[355] all'uso della tecnologia può essere identificato: nella semplificazione degli adempimenti tributari in materia di atti immobiliari, nell'automazione, con conseguente maggiore efficienza ed economicità, delle fasi di controllo, registrazione e voltura degli stessi atti, nell'ottimizzazione dei flussi informativi con gli uffici dell'amministrazione finanziaria, nella possibilità di registrazione contestuale all'invio dell'atto, quindi in maniera più veloce. Tutti vantaggi che hanno portato, seppure in maniera opportunamente frazionata nel tempo, a rendere obbligatorio per i notai l'uso di tale strumento entro il 2003.

In materia di pubblicità legale delle imprese, l'art. 31 comma 2-*ter* della l. 24 novembre 2000 n. 340 affida al notaio la facoltà di presentare attraverso un collegamento telematico, o su supporto informatico, al Registro delle imprese tutti i tipi di atti in materia societaria da lui rogati o autenticati. È l'attuazione del processo di informatizzazione di questo settore, iniziata dalla l. 29 dicembre 1993 n. 580, in materia di «riordinamento delle camere di commercio, indu-

[354] Oltre ad altre tipologie di atti (come ad esempio, per gli atti tra vivi, la costituzione e la cessione di diritti reali a titolo oneroso, le convenzioni amministrative ed edilizie, le affrancazioni, e, per gli atti *mortis causa*, l'accettazione, espressa o tacita, di eredità, l'ipoteca volontaria) a cui viene esteso, al momento a livello sia facoltativo che obbligatorio, l'utilizzo del modello unico dalle Circolari pubblicate recentemente.

[355] Le fonti che disciplinano tale procedura si individuano principalmente nel Decreto direttoriale 12 dicembre 2001, a firma congiunta Agenzia del Territorio, Agenzia delle Entrate e Dipartimento per gli affari di giustizia del Ministero di Giustizia, nella Circolare dell'Agenzia del Territorio e di quella delle Entrate n. 3 del 2 maggio 2002, nella Circolare n. 10 del 15 novembre 2002 dell'Agenzia del Territorio, nella Circolare dell'Agenzia delle Entrate n. 6 del 5 febbraio 2003, nel Decreto direttoriale del 18 aprile 2003 ed infine nella recentissima Circolare dell'Agenzia del Territorio n. 6 del 6 giugno 2003.

stria, artigianato e agricoltura», il cui art. 8 istituisce «presso la camera di commercio l'ufficio del registro delle imprese di cui all'articolo 2188 del codice civile». A fronte, infatti, della necessità di assicurare un'informazione veloce e sicura in materia societaria, abbandonando la modalità tradizionale dei fascicoli cartacei con capacità di circolazione praticamente inesistente, si è reso indispensabile fornire al gestore del sistema di pubblicità legale (l'ufficio del Registro delle imprese) le informazioni in formato digitale già dall'origine, garantendo la piena certezza legale delle medesime: certezza nella specie relativa alla provenienza e non ripudiabilità della dichiarazione, per l'assoluta regolarità formale e sostanziale dell'intero sistema, risultato raggiunto grazie alla firma digitale. Con l'introduzione del Registro telematico si verifica una drastica riduzione di tempi e costi: infatti, abolendo l'omologazione giudiziaria ed attribuendo al notaio il controllo di legalità degli atti delle società di capitali, l'iscrizione nel Registro avviene in tempi molto brevi, con particolare utilità per quelle realtà in cui l'iscrizione ha valore costitutivo.

Per meglio comprendere come poi in pratica il nuovo sistema di validazione legale dell'attività di documentazione elettronica riesca a dare fondamento giuridico a quelle attività del notaio che già in passato venivano gestite attraverso l'uso dell'elaboratore elettronico, si ritiene utile riportare un esempio relativo al ricevimento di un atto pubblico da parte del notaio[356], con le modalità stabilite nel D.P.R. 445/2000[357].

Si deve chiaramente 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 (alla luce delle recenti iniziative, lo stesso Consiglio Nazionale del Notariato). 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 stesse[358], attraverso questa volta una nuova modalità: in particolare, egli dovrà verificare la corrispondenza tra il *dispositivo di firma* e il titolare, e quindi constatare la validità della chiave pubblica della parte, e del relativo certificato[359]. 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, come si è appena visto, oramai svolte in via telematica), 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 digitale delle parti, momento in cui l'atto assumerà la veste definitiva[360]. La sottoscrizione dell'atto avverrà con le nuove modalità: così il notaio chiederà a ciascuna delle parti di apporre all'atto, in sua presenza, la loro firma digitale, utilizzando la funzione di *hash* e la loro chiave privata applicata all'impronta da questa risultante (nei modi già ricordati), di seguito alla quali apporrà poi a sua volta la propria firma digitale.

Il documento che ne risulterà sarà un testo crittografato, che potrà essere verificato con l'utilizzo della chiave pubblica del notaio sul-

[356] Così anche M. Miccoli, *Documento e commercio telematico*, IPSOA, Milano 1998, p. 108.

[357] A tale proposito si perdonino eventuali «inesattezze procedurali», sia dal punto di vista dell'attività professionale, sia da quello delle applicazioni tecniche che in questa sede vengono ipotizzate.

[358] In tal senso M.C. Andrini, *Dal tabellone al significato elettronico*, relazione al Convegno «Cyberlaw», Roma, 9 luglio 1998, p. 6.

[359] Volendo procedere nella nostra ipotesi, molto probabilmente il notaio, per verificare la validità dell'apparato tecnico usato dalla parte per firmare il documento informatico, prima lo farà usare, cioè farà usare sull'impronta del documento informatico la chiave privata della parte; quindi, vi applicherà 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, informazioni che il notaio avrebbe dovuto verificare collegandosi al certificatore del soggetto), per «aprire» il documento «firmato»; in caso di successo del procedimento, il notaio sarà quindi sicuro della validità di tale apparato. Altra più semplice modalità potrà essere invece connessa all'uso del dispositivo di firma: il notaio, identificata la parte con i mezzi tradizionali, verificherà direttamente 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 sempre il certificato del soggetto, contenuto nel dispositivo oppure collegandosi direttamente al certificatore del soggetto.

[360] Così M.C. Andrini, *op. cit.*, p. 2.

l'impronta di *hash*[361] del documento stesso, dal quale sarà poi possibile identificare con certezza sia il pubblico ufficiale che l'ha ricevuto, sia la sua qualifica e funzione[362]; 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 potranno avvenire in questo caso associando al documento elettronico principale un documento elettronico accessorio, munito ancora delle firme digitali di parti e notaio[363].

Concluso il momento di ricevimento dell'atto, il notaio passerà ad adempiere le 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. 13 del D.P.R. 445/2000, supporto che dovrà avere caratteristiche di non riscrivibilità e di inalterabilità, quali quelle oggi offerte dai dischi ottici, nella loro formula WORM[364]. Il notaio redigerà le copie dell'atto, sempre in maniera informatica, ai sensi dell'art. 20 del D.P.R. 445, apponendo, quindi, alle stesse la propria firma digitale (oggi firma elettronica qualificata) di seguito alla formula di conformità. Anche la trasmissione delle copie ai pubblici uffici avverrà nell'ambito della già ricordata 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 potranno, 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. 12 del D.P.R. 445, come ad esempio nel caso del sistema di pubblicità legale delle imprese[365]. Il notaio sarà infine esonerato dall'esibizione dell'originale, grazie al comma 3 dell'articolo 20 dello stesso D.P.R..

[361] 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, secondo la tecnica già esposta in precedenza.

[362] Utilizzando legittimamente una coppia di chiavi di crittografia asimmetrica di cui una certificato dal suo stesso Ordine professionale (il Consiglio Nazionale del Notariato nella sua funzione di ente certificatore accreditato), implicitamente si ha un riconoscimento del suo ruolo.

[363] Ancora M.C. Andrini, *op. cit.*, p. 2.

[364] Dischi ottici che è possibile incidere una sola volta, e non più modificare, mentre sarà poi possibile leggerli molte volte (*Write Once, Read Many*). Vedi in proposito i §§ 10, 18, 19, 157 e 252 del libro citato nella prefazione.

Analizzata la parte maggiormente applicativa di quella che si presume saranno le modalità operative dell'attività del c.d. *cybernotary*, sia dal punto di vista delle nuove applicazioni, sia da quello dell'attività tradizionale ma svolta con modalità nuove, approfondiamo ora il testo normativo che disciplina il sistema italiano delle firme elettroniche e di quelle digitali, con particolare riferimento alla figura del notaio.

219. *La disciplina normativa della firma digitale ed il notaio.* – Come principale punto di riferimento della nostra indagine si prenderà in considerazione il testo del D.P.R. 28 dicembre 2000 n. 445, che nel disciplinare in maniera unitaria la documentazione amministrativa, si occupa diffusamente del documento informatico.

In tale fonte la figura del notaio è presa in considerazione in diversi suoi articoli (in particolare gli artt. 13, 20 e 24), ma poi proprio in base a tale fonte è stata recentemente avviata una nuova realtà da parte della categoria dei notai, quella dell'attività di certificazione delle chiavi pubbliche degli appartenenti all'Ordine: diventando così elemento fondamentale della infrastruttura stessa della P.K.I. del nostro Paese[366].

[365] In cui il pagamento avviene *on line* mediante carta di credito secondo quanto stabilito dal Decreto del Ministero dell'economia e delle finanze 17 maggio 2002, n. 127 (il regolamento recante la disciplina delle modalità di pagamento dell'imposta di bollo dovuta sulle domande, le denunce e gli atti che le accompagnano, presentate all'Ufficio del registro delle imprese in via telematica, nonché la determinazione della nuova tariffa dell'imposta di bollo dovuta su tali atti) e dalla Circolare dell'Agenzia delle Entrate 7 agosto 2002, n. 67/E (che disciplina l'imposta di bollo su domande, denunce e atti che le accompagnano, presentate all'ufficio del Registro delle imprese per via telematica).

[366] Come si è detto, dal 12 settembre 2002 il Consiglio Nazionale del Notariato è diventato il quindicesimo certificatore dell'elenco pubblico gestito dall'A.I.P.A., come si può ancora leggere nel sito dell'Autorità (oggi sostituita dal Dipartimento per l'innovazione e la tecnologia), all'indirizzo *http://www.aipa.it/attivita[2/certifica[17/* consultato il 24 febbraio 2003.

Le maggiori difficoltà nell'integrazione tra funzione notarile ed il nuovo sistema di validazione giuridica della documentazione elettronica si sono avute con riferimento alla figura della *firma digitale autenticata*, disciplinata originariamente dall'art. 16 DPR 513/1997. In particolare, tale figura mal si conciliava con la struttura stessa dell'intero sistema, analizzata nei precedenti paragrafi. Infatti, da una parte si pone la coppia di chiavi di crittografia asimmetrica, di cui una privata, segreta e presuntivamente strumento efficace per l'attribuibilità soggettiva del documento informatico, ed una pubblica, necessaria per risalire all'autore dello stesso; dall'altra, invece, è la certificazione della chiave pubblica da parte di un soggetto terzo, in possesso di specifici e stringenti requisiti stabiliti dalla legge, che permette di associare con certezza le due chiavi al soggetto titolare: tutta questa costruzione rende di per sé non ripudiabile un determinato documento informatico, e quindi non disconoscibile una determinata scrittura privata. E di conseguenza inutile l'autentica notarile. Tra l'altro è proprio la disciplina stabilita nell'art. 24 che, prevedendo un'attività (la sottoscrizione digitale fisicamente davanti al notaio) troppo legata alla realtà «cartacea», e soprattutto in sostanziale contrasto con il funzionamento dello stesso, la rende di difficile integrazione nelle nuove modalità[367].

Nonostante la vivace polemica basata, almeno parzialmente, sulle considerazioni appena esposte, la norma discussa è stata poi ripresa integralmente nell'art. 24 del DPR 445/2000[368]: può, quindi, essere

[367] Infatti il sistema creato dal legislatore del 1997 prescindeva proprio dal considerare la possibilità che la chiave privata, necessaria per ricostruire la provenienza del documento, non l'abbia il suo titolare (*ratio* legata alla necessità della presenza del pubblico ufficiale): altrimenti, sulla base di questa eventualità, non si sarebbe potuto attribuire alcun valore al documento informatico al di fuori della fattispecie prevista, ed anzi tutti i documenti informatici sottoscritti con firma digitale avrebbero dovuto essere autenticati.

[368] Art. 24: «*1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato; 2. L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, n. 1 della legge 6 febbraio 1913, n. 89; 3. L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti; 4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 20, comma 3; 5. Ai fini e per gli effetti della presentazione di istanze agli organi della pubblica amministrazione si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni; 6. La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposte la firma digitale e la validazione temporale a norma del presente testo unico*».

utile riportare l'opinione di una dottrina che considera la figura controversa come un «*plus* rispetto alla possibilità per le parti di scambiare le proprie dichiarazioni attraverso un supporto telematico, né più né meno come l'art. 2703 c.c. è una forma di guarentigia rinforzata rispetto alla forma debole del documento di cui all'art. 2702 c.c. La sua *ratio* deve essere poi cercata, oltre che nell'ambito dell'amministrazione pubblica del diritto privato, nel potere di modifica dei registri pubblici da parte dell'atto notarile e nell'aumentata necessità di assicurare garanzie di certezza nel momento in cui i traffici giuridici hanno assunto la velocità conseguente all'uso dei nuovi strumenti»[369].

Oltre alla previsione della firma digitale autenticata, il D.P.R. 445 considerava l'attività notarile nell'ambito della fattispecie del deposito della chiave privata di un soggetto[370]. A tale proposito occorre ricordare come il sistema della crittografia asimmetrica si basi su una coppia di chiavi, strumenti di criptazione che svolgono ciascuna una diversa finalità, e che vengono utilizzate in diversa maniera: la chiave pubblica, usata in genere da chi vuole inviare, o conservare, messaggi in modo da permettere al solo titolare della corrispondente chiave privata di leggere tali messaggi; quella privata, applicata al documento

[369] «Come nel lontano 1913 un legislatore accorto previde la possibilità di redigere l'atto notarile per telegrafo, purché le parti distanti fossero, ciascuna, assistite da un notaio che attestasse la legittima provenienza della dichiarazione, oggi l'art. 16 del DPR 513/97 chiama il notaio ad essere custode ed artefice del documento elettronico»: così M.C. Andrini, *Dal tabellone al sigillo elettronico*, relazione al Convegno «Cyberlaw», Roma, 9 luglio 1998, p. 9.

[370] Art. 26: «*1. Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata presso un notaio o altro pubblico depositario autorizzato; 2. La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e deve essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni; 3. Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili*».

per rendere certa l'attribuibilità dello stesso al suo autore. Per questi motivi risulta differente anche la gestione delle due chiavi: quella pubblica dovrà essere diffusa il più possibile, mentre all'opposto per quella privata la conservazione dovrà essere riservata al massimo[371].

La disciplina della diffusione del primo tipo di chiavi è legata all'attività di certificazione (su cui si veda gli artt. 27 e ss. del D.P.R. 445), mentre quella relativa alla chiave privata è stabilita proprio dall'art. 26, secondo cui la chiave privata può essere depositata, in forma segreta, «presso un notaio o altro pubblico depositario autorizzato», seguendo la disciplina stabilita dall'art. 605 c.c. relativamente alle formalità necessarie per il deposito di un testamento segreto. Tale attività, a differenza della pubblicazione della chiave pubblica, risulta facoltativa. Le finalità che possono spingere a svolgerla sono individuabili nel desiderio di adottare una modalità sicura di conservazione, oltre alla costruzione preventiva della prova di essere, o di essere stato in un determinato tempo[372], il titolare di quella chiave. A fronte di tali utilità si deve però preventivare una procedura, quella dell'art. 605 c.c., un po' troppo complessa, e comunque di non chiara adattabilità ad un oggetto (un documento elettronico corrispondente alla chiave privata) di natura e funzionalità ben diversa rispetto al testamento (cartaceo) segreto.

Altra considerazione delle funzioni notarile avviene, come si è detto nell'art. 20, comma 3, del D.P.R. 445, in materia di copia di atti e documenti informatici[373], che rende necessaria l'attestazione del

[371] Derivando dall'uso della chiave privata la generazione di una firma digitale, che lega indissolubilmente un determinato documento non già al suo autore, quanto al titolare della stessa (che in linea di massima sarà poi anche l'autore del documento, ma la corrispondenza non è assoluta: si immagini l'eventualità che il titolare della chiave privata la smarrisca, o gli venga sottratta), o meglio al titolare della coppia di chiavi, sarà un importante onere dello stesso la sua conservazione sicura e riservata, adottando «tutte le misure organizzative e tecniche», anche al fine di «evitare danno ad altri» (art. 28, comma 1, D.P.R. 445: si pensi al danno conseguente alla conclusione di un contratto con chi non è poi quella determinata parte con cui si pensava di aver instaurato la trattativa, il risarcimento del quale potrebbe essere richiesto al titolare della chiave privata inadempiente agli obblighi di custodia della stessa).

[372] Si pensi alla previsione dell'art. 8, comma 2, del D.P.R. 445/2000, che richiede il deposito presso il certificatore minimo per 10 anni, ma che nulla dispone relativamente all'eventuale periodo superiore, in cui l'utente si può trovare in difficoltà per dimostrare la titolarità di una determinata chiave: il deposito della chiave privata presso un notaio permetterebbe di usufruire di un valido ausilio.

[373] Art. 20: «*1. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se*

notaio relativa alla 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. In questo caso la norma in commento, che disciplina tutte le vicissitudini relative alla trasferibilità del documento da un supporto ad un altro, dal *medium* digitale a quello cartaceo e viceversa, nonché gli aspetti relativi agli obblighi di conservazione e di esibizione di documenti, soffre di un'impostazione concettuale errata. Infatti con riferimento al documento informatico, ed alla sua struttura in *bit*, risulta impossibile, a fronte della completa riproducibilità della sequenza di informazioni binarie che costituiscono il contenuto di un determinato documento, distinguere l'originale dalla copia: anzi, «la stessa nozione di originale, e quella correlata di copia, perdono di significato»[374]. Invece la norma in commento sembra dettata per una realtà ancora troppo «cartacea», e sottopone, quindi, la copia del documento informatico agli stessi requisiti richiesti per il supporto più tradizionale.

Ed è proprio il riferimento al «supporto» a permettere un corretto inquadramento della disposizione fra quelle che hanno disciplinato il documento prodotto attraverso l'elaboratore da un punto di vista «statico» (cioè a prescindere da una sua comunicazione a distanza attraverso applicazioni telematiche): il cui principale riferimento

conformi alle disposizioni del presente testo unico; 2. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata da parte di colui che li spedisce o rilascia una firma elettronica qualificata; 3. Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche di cui all'articolo 8, comma 2; 4. La spedizione o il rilascio di copie di atti e documenti di cui al comma 2 esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge; 5. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate nell'articolo 8, comma 2».

[374] Così M. Minerva, *L'attività amministrativa in forma elettronica*, in *Il Foro amm.*, 1997, IV, p.1311, che suggerisce più opportuno l'uso del solo termine «duplicato».

si può trovare nell'art. 2220 del codice civile[375], rispetto al quale l'art. 20 del D.P.R. 445/2000 amplia e rende maggiormente fungibile la nozione di «documento informatico», e la separa dalla necessità della sua conservazione su «supporti di immagine»[376], permettendola su supporti elettronici in genere, purché firmati digitalmente ai sensi dello stesso decreto. Le diverse fattispecie previste nell'art. 20, a fronte di un'affermazione generica contenuta nel comma 1, che replica l'art. 8 comma 1 dello stesso D.P.R. 445 riferito al documento informatico, sono così schematizzabili:

– duplicati, copie o estratti di un documento informatico, conformi alla disciplina del Regolamento, su qualunque supporto, «sono validi e rilevanti a tutti gli effetti di legge»[377];

– atti pubblici, scritture private e documenti in genere (compresi atti e documenti amministrativi di ogni tipo), spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali (artt. 2714 e 2715 c.c.), possono essere contenuti con piena efficacia in documenti informatici se firmati digitalmente da colui che li spedisce o rilascia, ed a prescindere dalla produzione o esibizione dell'originale, dalla quale si è esonerati;

– documenti formati in origine su supporto non informatico, e quindi essenzialmente su quello cartaceo, possono essere sostituiti «ad ogni effetto di legge» da copie informatiche, se la conformità all'originale di queste ultime è autenticata da un notaio o altro pubblico ufficiale autorizzato a tale attività[378].

[375] Il cui terzo comma, introdotto dall'art. 7-*bis* del D.L. 10 giugno 1994, n. 357, convertito nella L. 8 agosto 1994, n. 489, testualmente recita: «*Le scritture e i documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti*».

[376] Vedi in proposito i §§ 15 e 19 del libro citato nella prefazione.

[377] Lascia qualche perplessità la locuzione «anche se riprodotti su diverso tipo di supporto» che si trova nel testo della norma: diverso rispetto a quello informatico? Quindi anche quello cartaceo? Ipotesi un po' dubbia da un punto di vista tecnico, riuscendo difficile immaginare come riprodurre su carta la sequenza di *bit* che costituisce un suono. Più opportuna sembra l'interpretazione adottata nel testo, che considera tale locuzione il mezzo per ampliare le tipologie dei supporti digitali su cui conservare i documenti informatici: non solo quelli di «immagine», ma anche quelli magnetici, magneto-ottici, digitali in genere.

[378] In questo caso l'autenticazione avviene, ai sensi del comma 3 dell'articolo in commento, «con dichiarazione allegata al documento informatico e *asseverata* secondo le regole tecniche di cui all'art. 8, comma 2».

Le applicazioni pratiche di tali disposizione sono in fase di concreta attuazione, come si è detto nelle pagine precedenti proprio con riferimento all'attività documentatrice del notaio.

Ultima norma del D.P.R. 445/2000 ad essere presa in considerazione è l'art. 13, anche in questo caso riferita essenzialmente agli aspetti «statici» del documento informatico, ed a quelli relativi alla conservazione dello stesso, a prescindere dalla sua ulteriore trasmissione a distanza[379]. Rispetto a tale argomento viene presa in considerazione, in particolare, la conservazione dei «libri obbligatori e delle altre scritture contabili» quando sono rappresentate da documenti informatici. Nonostante la precedente produzione normativa sulla fattispecie, vincolata in ogni caso alla mediazione tra l'esigenza di certezza ed inviolabilità della documentazione necessaria a fini fiscali, con la prassi relativa alla sua conservazione, e condizionata comunque dal livello della tecnologia, la norma in commento conserva intatta la sua importanza. Questo perché consente anche, proprio sulla base della metodologia informatica impiegata, di prescindere da supporti particolari: sarà infatti l'uso della crittografia asimmetrica, e quindi la tecnologie relativa alla modalità di formazione del documento elettronico, a rendere certa ed inviolabile la documentazione conservata nelle memorie ausiliarie di un sistema di elaborazione dati, e non la tecnologia relativa al supporto.

Si conclude, con l'esame della disciplina relativa alla tenuta di libri e scritture attraverso il mezzo informatico, la parte del presente scritto relativa all'impatto dell'informatica sulla prova documentale, attraverso la quale si è potuto «toccare con mano» come la capacità fortemente rivoluzionaria delle nuove tecnologie porti non già ad un appiattimento delle peculiarità umane, ma ad una loro esaltazione nell'efficienza e nell'innovazione: e di conseguenza la nascita di nuove applicazioni e di nuove realtà che, come si è più volte sottolineato, debbono essere conosciute ed esaminate con l'attento sguardo del giurista. Come per l'impatto dell'informatica nel mondo del lavoro, argomento del prossimo capitolo.

[379] Art. 13: «*I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente regolamento e secondo le regole tecniche definite col decreto di cui all'articolo 8, comma 2*».

Sezione II

Ulteriori considerazioni sul tema del documento informatico e sulla firma elettronica

220. *Innovatività dirompente del documento informatico e della firma elettronica in tutto l'ordinamento giuridico e, in particolare, nel diritto civile.* – Se è vero che in tutto il nostro ordinamento giuridico e, in particolare nel diritto civile (oltreché in quello amministrativo), riveste massima importanza l'atto scritto e la sua sottoscrizione autografa solo grazie alla quale l'atto stesso diventa imputabile ad un determinato soggetto che assume, ad ogni effetto, la responsabilità del suo contenuto, allora dovranno considerarsi di pari importanza le norme di legge recentemente emanate per effetto delle quali diventa giuridicamente e pienamente rilevante un tipo nuovo di documento – il «documento informatico» – e un tipo nuovo di sottoscrizione: la firma elettronica.

L'importanza di tale novità ci sembra tale e tanta da ravvisare in essa il riflesso forse più rivoluzionario dell'irruzione dell'informatica in tutta la nostra vita e, quindi, inevitabilmente nel campo del diritto.

La prospettazione di tale novità ci induce, inoltre, a premettere tutta una serie di considerazioni che ci paiono di estremo interesse per ogni giurista e in particolare per il civilista.

La prima di esse è che non può più considerarsi tale chi si ostini a non volersi interessare dell'informatica e a non volerne capire l'intima essenza: il che non vuol dire farne necessariamente uso pratico personale, ma, indipendentemente da esso, comprendere in che cosa consista e perché e come possa servire a migliorare la qualità della vita e, a tal fine, esser presa in considerazione dal diritto. Un giurista, un civilista, che si rifiutasse ancora di fare questo sforzo, si porrebbe allo stesso livello di chi volesse comprendere il diritto senza saper leggere e scrivere.

221. *La registrazione dei BIT nelle memorie del computer: è «scrittura»?.* – La seconda considerazione preliminare che le norme in esame ci sospingono a fare riguarda il problema, fondamentale per qualsiasi giurista, del significato delle parole di cui la legge è costituita e la facilità con cui l'interprete può falsarlo per superficialità, per mancanza di conoscenze storiche, per difetto di spirito critico. Infatti, fin da quando, intorno al 1960, si cominciarono a registrare

nelle memorie del computer, veri e propri testi scritti (e non semplicemente numeri, nomi e indirizzi), ci si chiese subito se tale registrazione potesse considerarsi «*scrittura*» in senso tecnico giuridico, indipendentemente dal fatto che detto testo potesse poi venir stampato su un foglio di carta (c.d. «tabulato») dallo stesso computer in fase di «output». E, nella maggioranza dei casi, lo si negò sul rilievo che la semplice registrazione di segni elettronici (i BIT chiamati convenzionalmente 0 ovvero 1, a seconda che significassero presenza o assenza di corrente elettrica) su un supporto ben diverso dalla carta (quale può essere un circuito monolitico in una memoria elettronica in senso stretto, ovvero una superficie magnetizzabile o smagnetizzabile come nelle memorie magnetiche ovvero un compact-disc opportunamente perforato da un raggio laser come nelle memorie c.d. «ottiche») non potesse mai considerarsi scrittura agli effetti giuridici mancando, oltre alla stabilità dei segni registrati, il supporto indefettibile della carta che la scrittura necessariamente implica e mancando, inoltre, la possibilità di sottoscriverlo con firma autografa.

Raramente i giuristi commisero tanti errori – e di varia natura – nell'esprimere un siffatto giudizio negativo. Dimenticarono, innanzitutto, che l'uomo cominciò a scrivere, prima ancora che sulla carta, sulla pietra, sulla terracotta, sulle tavolette cerate, sul cuoio, sulle foglie di papiro, sulla pergamena e, appena da cinque secoli, sulla carta. Trascurarono, inoltre, di considerare che i BIT non sono sempre volatili (come lo sono quelli registrati sui circuiti elettronici a mezzo dei c.d. «chips»), ma possono essere anche stabili (come quelli registrati su memorie magnetiche, anche se cancellabili) *e addirittura indelebili* molto più di quanto non lo siano quelli vergati sulla carta, come ad esempio, quelli registrati sui compact-disc («C.D. ROM») per effetto di una serie di perforazioni ablatorie eseguite con un raggio laser sul fondo dei suoi solchi concentrici. Sfuggì loro che i BIT, codificati in combinazioni convenzionali, costituivano *un nuovo alfabeto* con cui era possibile esprimere qualsiasi parola, che il flusso degli elettroni utilizzato per far loro assumere e variare il valore di zero o di uno costituiva una sorta di *nuovo inchiostro*, che, infine, i circuiti, le superfici, il fondo dei solchi sui quali i BIT venivano memorizzati, costituiva *il nuovo possibile supporto* su cui farli apparire, cioè una sorta di nuovo tipo di carta. Ignorarono che anche una firma autografa può ben essere registrata nelle memorie di un computer (e riprodotta poi in output perfettamente uguale all'originale) come se si trattasse di un disegno, in quanto il computer può essere dotato,

oltreché di una tastiera di segni alfanumerici, anche di una lavagna elettronica su cui tracciare con una speciale penna (la «ligth pen») qualsiasi figura e, quindi, negarono che quanto archiviato in BIT nelle memorie di un computer potesse esser considerato una nuova forma di scrittura più per misoneismo (anche se inconsapevole) che non per fondate argomentazioni.

222. *Il tramonto della firma autografa.* – Il progresso (sia esso morale e/o tecnologico) ha una sua forza irresistibile, inesorabile che, da un lato, ha costretto il legislatore a riconoscere espressamente la nuova figura giuridica del «documento informatico» (come nell'art. 491-bis del c.p. introdotto dalla l. 23 Dicembre 1993 n. 547), dall'altro lato ha screditato sempre più nell'opinione pubblica il convincimento dell'importanza e della affidabilità della firma autografa in calce a documenti formati meccanicamente, tantoché, in talune specie di essi, detta firma, ridotta progressivamente, specie su taluni atti, ad una semplice sigla o ad un'indecifrabile scarabocchio, è finita addirittura con lo sparire silenziosamente e completamente senza che il pubblico quasi se ne accorgesse. Così è avvenuto, ad esempio, ormai già da qualche anno, per le ricevute dei versamenti di denaro in conto corrente postale, che recano in calce una semplice stampigliatura meccanica degli estremi identificativi del versamento senza più alcunché di vergato a mano: e nessuno se n'è lamentato.

È iniziato così il tramonto dell'affidabilità e dell'importanza della sottoscrizione autografa (cioè di uno dei pilastri dell'ordinamento) dovuto, in sintesi, alla constatazione che:

a) se la firma autografa viene disconosciuta, il responso circa la sua autenticità è affidato ad un perito calligrafo il cui esame è basato su una scienza che, quale è la grafologia, non tutti ritengono costituire una scienza esatta e infallibile (in senso galileiano): un giudizio analogo a quello sull'autenticità dei quadri pittorici, molto spesso discutibile;
b) la firma autografa non garantisce l'integrità del testo sottoscritto (caso limite, ma non raro: il foglio firmato in bianco);
c) proprio l'uso del computer renderebbe oggi relativamente facile la falsificazione di qualsiasi firma, difficilmente smascherabile perché realizzata in applicazione di quelle stesse regole (o «algoritmi» che dir si vogliano) delle quali il grafologo si serve per verificarne l'autenticità;
d) stando alla più comune esperienza non è affatto vero che l'autografia sia facilmente riconoscibile (talvolta neppure la propria!) specie dai terzi anche se muniti di uno «specimen» di confronto;
e) paradossalmente mancano norme precise sul modo di firmare. La firma – e in specie la sottoscrizione- dovrebbe essere sempre leggibile: altrimenti come contestare, ad esempio, che una persona abbia voluto firmare per un'altra? Eppure, molto spesso le firme non sono leggibili. Nelle copie degli atti amministrativi si legge, infatti, scandalosamente: «F.TO ILL.BILE». Giurisprudenza costante si è formata solo nell'escludere la validità di una firma con caratteri «a stampatello». Così si è pervenuti ad ammettere come firma, senza quasi accorgersene della gravità, anche semplici scarabocchi;
f) quando la firma deve essere ripetuta tante volte (ad es. su ogni foglio di atti dal testo lunghissimo) diventa notoriamente, anche quando permane formalmente autografa, un fatto tanto meccanico da non garantire affatto che chi l'ha apposta abbia preliminarmente letto il contenuto dei fogli e abbia voluto asseverarlo. Si è giunti, così, in taluni casi, all'assurdo della «firma a stampa» (come quella del Governatore della Banca d'Italia sulla vecchia carta-moneta o quella del Sindaco del Comune sui certificati elettorali): compiendo, così, una sorta di cammino a ritroso nella storia della diplomatica, tornando dalla firma autografa al timbro o al sigillo.

Come accade per le persone e per le istituzioni che, quando non svolgono più una funzione utile agli altri, vengono – o prima o poi – prima accantonate e poi addirittura del tutto dimenticate, così sta accadendo per la firma autografa: la firma elettronica la sta a poco a poco soppiantando, non perché il nuovo sia sempre destinato a soppiantare il vecchio, ma perché è il vecchio stesso che decreta la sua morte smettendo di funzionare e di apparire utile[380].

223. *I primi passi del legislatore verso il riconoscimento del documento informatico come documento scritto.* – La firma elettronica, che il decreto legislativo in esame prevede e regola, oltre a farci ricordare, in linea di principio, come e perché il nuovo soppianta il vecchio, serve anche emblematicamente a farci riflettere sul difficile e

[380] In proposito vedi anche la nota n. 62 al § 120.

dubbioso cammino che il legislatore ha, da oltre un decennio a questa parte, intrapreso per innestare l'informatica sul tronco tradizionale del diritto e per offrire, quindi, ai problemi giuridici nuove e più appaganti soluzioni.

Infatti, dapprima con il d.lgvo 12 Febbraio 1993 n. 39 (art. 3), il legislatore, forse per effetto dell'impressione riportata nel constatare che sulle ricevute dei versamenti in conto corrente postale la firma autografa del cassiere ha, silenziosamente e senza alcun inconveniente o protesta, lasciato il posto ad una semplice stampigliatura meccanica recante gli estremi del versamento eseguito, estese la possibilità di *sostituire* la firma autografa del funzionario della P.A., responsabile del contenuto degli atti formati o trasmessi tramite il computer, con la semplice indicazione a stampa del suo nome. Solo in un secondo momento «re melius perpensa», si rese conto che tale soluzione era troppo semplicistica in quanto chiaramente inidonea a fornire adeguate garanzie di autenticità e, quindi, di validità degli atti e che al fugace riconoscimento del documento informatico, peraltro in una norma penale (il già citato art. 491-bis del c.p. introdotto con la l. 23 Dicembre 1993 n. 547 sulla criminalità informatica) occorreva far seguire una ben più organica disciplina che desse una più precisa definizione del documento informatico e, al tempo stesso, risolvesse convenientemente il problema di come assicurarne la imputabilità giuridica a tutti gli effetti.

Si pervenne, così, ad emanare una serie di disposizioni di fondamentale importanza e di straordinaria carica innovativa quale quelle contenute nel comma 2 dell'art. 15 della l. 15 Marzo 1997 n. 59 (c.d. «legge Bassanini») e nel pedissequo regolamento approvato con il D.P.R. 10 Novembre 1997 n. 513. Nel summenzionato comma 2 si stabilì che: «Gli atti, dati e documenti formati dalla P.A. e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge». Nel D.P.R. 10 Novembre 1997 n. 513 si precisò:

- all'art. 1 che «per documento informatico si intende la *rappresentazione* informatica di atti, fatti o dati giuridicamente rilevanti», così immutandone la definizione già datane nell'art. 491-bis c.p. ove, invece, è detto che «per documento informatico si intende qualunque *supporto* informatico...»: e dell'importanza della sostituzione del termine «supporto» con quello ben diverso di «rappresentazione» parleremo dopo;

- all'art. 4 che «il documento informatico, munito dei requisiti dal presente regolamento, *soddisfa il requisito legale della forma scritta*»;
- all'art. 5 che «il documento informatico, *sottoscritto con firma digitale*, ha efficacia di scrittura privata ai sensi dell'art. 2702 c.c.»;
- all'art. 10 che «l'apposizione della *firma digitale* al documento informatico, equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo»;
- all'art. 19 che: « in tutti i documenti informatici della P.A. la firma autografa o la sottoscrizione comunque prevista è sostituita dalla *firma digitale*».

Dalle norme surriportate emerge che occorsero al legislatore alcuni anni per rendersi conto innanzi tutto, che l'uso dei BIT costituiva una forma di vera e propria scrittura, anche se nuova, come era stato sostenuto da una parte delle dottrina, anche se minoritaria. Il fatto che quest'ultima avesse evidenziato che i BIT costituivano un nuovo alfabeto, il flusso degli elettroni un nuovo inchiostro e i circuiti elettronici, i nastri magnetici, i compact-disk nuovi tipi di supporti materiali sui quali scrivere induce, infatti, a interpretare le norme sopraripportate come il riconoscimento della giustezza di tale tesi, volta a chiudere definitivamente la diatriba sul valore giuridico della registrazione dei dati in BIT nelle memorie del computer: vera e propria «scrittura» e non semplicemente una «fictio iuris» imposta per attribuire a tale registrazione un valore che per sua natura non avrebbe. Se per scrittura, infatti, deve intendersi, dal punto di vista storico e funzionale, l'impronta non volatile di determinati segni convenzionali, su qualsiasi materiale e con qualsiasi strumento, tali da rendere possibile la lettura a distanza di tempo e di luoghi e, quindi, come mezzo di trasmissione del pensiero a persone anche lontane nel tempo e/o nello spazio, non sussiste alcuna seria ragione per ostinarsi a negare, più che la *equivalenza* della registrazione in BIT alla scrittura, l'*identità* dell'una rispetto all'altra.

224. *La riproduzione informatica della firma autografa.* – Ciò non toglie, ovviamente, che tale registrazione abbia peculiarità sue proprie nuovissime rispetto alla scrittura tradizionale come, innanzitutto, quella della *libera scorporabilità* dei segni registrati sul supporto dal supporto medesimo: mentre, infatti, fino a prima del computer, i segni memorizzati non si potevano scorporare dal materiale su cui

essi erano stati impressi, i BIT, invece, possono essere prelevati da esso con la massima naturalezza e travasati su uno diverso, alla stessa stregua dei liquidi che possono essere travasati da un recipiente ad un altro. Per comprendere tale originalissima caratteristica dei BIT il legislatore ha impiegato quattro anni: mentre, infatti, nella legge del 1993 n. 547 (che ha portato all'introduzione dell'art. 491 bis del c.p.) il documento informatico viene definito come «*supporto*» dei BIT in esso registrati, nella legge Bassanini del 1997 (n. 59), il medesimo documento viene definito come «*rappresentazione*» informatica di atti o fatti, senza più alcun accenno al supporto che, a causa della libera travasabilità dei BIT, non ha più alcun decisivo valore.

Non si tratta soltanto di una maggiore precisione terminologica: il legislatore del 1997, infatti, ha anche compreso, sia pure implicitamente, che, su un documento informatico, la sottoscrizione costituita dalla indicazione del proprio nome e cognome, *ancorché autografa*, come suggello di una dichiarazione a lui imputabile, non è affidabile, non perché non sia tecnicamente memorizzabile e riproducibile in output (come erroneamente ritenevano gran parte dei vecchi giuristi, ignari del fatto che il computer può essere dotato, come organo di input, anche di una «graphic tablet» su cui tracciare con una «light-pen» qualsiasi disegno e, quindi, anche una firma autografa, ottenendone così in output la perfetta riproduzione a mezzo di una stampante a getto d'inchiostro), ma *perché tale firma, apposta in calce a un determinato documento, può benissimo essere prelevata da esso e «travasata» in calce ad un altro*, con una tecnica alla portata di tutti gli utenti del computer e da essi oggi evocata con l'espressione metaforica «stacca e incolla altrove».

Il legislatore, quindi, si è reso ben conto che, data tale libera «travasabilità», la sottoscrizione del documento informatico, per garantire l'imputabilità del testo soprastante, non poteva più essere costituita dalla indicazione, sia pure autografa, del nome del dichiarante, ma doveva consistere in ben altro, in un «quid» che ha sì continuato a chiamare ufficialmente «firma» (come nelle espressioni «firma digitale» e «firma elettronica»), ma ciò al solo scopo di dare al pubblico il senso della *continuità funzionale* tra il vecchio e il nuovo, cioè per rendere chiaro che anche i nuovi tipi di firma servono per garantire l'imputabilità dello scritto, così come la garantiva la firma autografa.

225. *La firma digitale: caratteristiche e funzione essenziali. Chiave privata e chiave pubblica: un sigillo, non una firma.* – Le nuove firme,

infatti, da un punto di vista ontologico, *non* hanno nulla a che vedere con una firma in senso tradizionale, *non riproducono il nome e il cognome di nessuno, non* sono parole, né disegni, *non* hanno, quindi, nulla a che vedere con l'autografia e neppure con la grafia (cioè con le caratteristiche proprie della scrittura a mano, rivelatrici dell'identità di chi scrive). Se proprio si vuol trovare una analogia col passato, si può dire che la firma digitale o elettronica è più simile ad un *sigillo* (di metallo o di cera-lacca) che non ad una firma.

Non staremo qui a descrivere analiticamente in che cosa consista la *firma digitale* menzionata nelle norme sopraripportate essendo stato già illustrato nella sezione del capitolo che precede (Vedi tra l'altro per un esempio dettagliato di firma digitale il § 31 del libro citato nella prefazione). Tralasciamo anche di ripetere quanto ivi già detto sulla preliminare operazione di compressione del testo da criptare, chiamata «hash» che dà luogo alla c.d. «impronta digitale» del testo stesso. Qui basterà tener presente che:

a) il dichiarante cripta lo scritto che vuole essergli imputato con un codice segreto, a conoscenza del solo dichiarante e che, per tale motivo, viene chiamato «*chiave privata*». Lo spedisce quindi, telematicamente al destinatario;
b) tale messaggio può essere decriptato solo in base ad un codice *diverso* da quello segreto usato dal mittente anche se connesso ad esso mediante un algoritmo matematico difficilissimo a ricostruirsi, sicché la decriptazione riesce solo se, in applicazione di tale algoritmo, risulti correlativo al codice segreto del mittente. Questo codice *diverso* (di cui si serve il destinatario del messaggio per decriptarlo) è chiamato dal legislatore «*chiave pubblica*» perché tutti possono conoscerlo chiedendo ad un determinato terzo, fidefaciente precostituito, quale sia il codice necessario per decriptare i messaggi inviati da una certa persona. Se il mittente avrà avuto cura di depositare la sua «*chiave pubblica*» presso tale terzo fidefaciente, quest'ultimo potrà comunicarla al destinatario, garantendogli che essa è quella propria del mittente e di nessun altro sicché è riferibile solo a lui;
c) mediante l'uso della chiave pubblica del mittente (venuta in tale modo a conoscenza del destinatario) quest'ultimo riuscirà a decriptare il messaggio ricevuto *solo* se corrisponda alla chiave segreta usata dal mittente per criptarlo, anche se – è utile ripeterlo – tale corrispondenza non permetterà mai di risalire

alla predetta chiave segreta, salvo che non si disponga di un computer potentissimo quali pochi ce ne sono al mondo e lo si usi ininterrottamente a tale fine per alcuni mesi tanti sono i calcoli che sarebbe necessario fare. È tale impossibilità pratica di *risalita* da una chiave all'altra che si vuol mettere in luce quando si definiscono, come nell'art. 1 lett. d del D.P.R. 513 del 97, «asimmetriche» le due chiavi che devono coesistere e appartenere ad un unico e medesimo soggetto per far funzionare il sistema della firma digitale[381];

d) per effetto della conseguita decriptazione del messaggio mediante uso di una chiave (pubblica) che un terzo fidefaciente *certifica* essere appartenente ad una determinata persona, il destinatario potrà con certezza imputare a quest'ultima il messaggio ricevuto: il mittente non potrà più ripudiarlo, cioè contestare che promani da sé, in quanto *sua* – e soltanto sua – è la chiave privata con cui egli ha criptato il messaggio e sua – e soltanto sua – è la correlativa chiave (pubblica) che ne ha consentito la decriptazione. In tal modo la «firma digitale» assolve pienamente la funzione di *imputabilità* dello scritto, per secoli svolta mediante la sottoscrizione autografa;

e) la «firma digitale», quindi, non è un modo criptico per indicare le parole corrispondenti al nome e al cognome del dichiarante e impedire che esse siano ricopiate in fac-simile autografo in calce ad altri scritti e – meno che mai – basa la sua affidabilità sulla eguaglianza (anche se più o meno approssimata, ma pur sempre rivelatrice dei caratteri costanti della grafia di una certa persona) delle firme apposte da essa su tanti documenti diversi, ma costituisce una *derivazione matematica*, compattata e criptata, *di un determinato testo scritto*, quale che ne sia stato il suo vero autore, sicché ogni *testo diverso* anche per un solo particolare (quale può essere, ad es., un segno di punteggiatura) avrà una firma digitale *diversa* anche se proveniente dal medesimo autore. Ecco perché la «firma digitale» assicura *non solo l'imputabilità* certa dello scritto cui si riferisce, *ma anche la sua integrità e genuinità*: nessuna alterazione, neppure minima, ne sarà più possibile e si rende addirittura inconcepibile la c.d. sottoscrizione di un foglio in bianco. Sotto questo aspetto, la firma digitale assicura una funzione in più rispetto a quella svolta dalla firma autografa tradizionale, idonea soltanto a garantire l'imputabilità dello scritto soprastante, ma non già l'assenza di postume correzioni , cancellazioni o aggiunte: dimostrazione lampante questa che l'innesto dell'informatica sul vecchio tronco del diritto non solo consente le stesse garanzie che esso dà, *ma ne dà di maggiori*, riuscendo, così, a tutelare meglio che in passato i valori fondamentali dell'ordinamento.

[381] Si tenga presente che la lunghezza minima delle chiavi è stabilita in 1024 bit.

Infatti, eliminare le incertezze che sempre può dare il riconoscimento dell'autografia specie da parte dei terzi e, quindi, l'imputabilità del testo dei documenti e/o il sospetto che il testo sottoscritto sia stato successivamente e arbitrariamente ritoccato costituiscono valori (quali la facilitazione dei negozi, la lotta agli inganni, la tutela della buona fede) che l'ordinamento avrebbe voluto, certamente e fin da sempre, tutelare, ma che, prima dell'avvento del computer, *non riusciva a garantire* per difetto dei mezzi tecnici adeguati. Grazie all'informatica, tali mezzi oggi sono disponibili e il legislatore, quindi, non poteva esimersi dal consentirne e favorirne l'uso. E solo grazie ad essi decollerà il c.d. *commercio elettronico* – tante volte annunciato, ma ancora di modeste dimensioni – che dovrebbe realizzare quella new-economy dalla quale molti si aspettano un nuovo miracolo economico.

226. *Differenza delle chiavi asimmetriche rispetto a quelle simmetriche.* – Il sistema della firma digitale può apparire alquanto complicato. Per comprendere le ragioni per le quali il nostro legislatore lo ha prescelto, occorre riflettere adeguatamente sulla *duplicità* delle chiavi (privata e pubblica) su cui è basato e sulla loro c.d. «asimmetricità».

Fino a prima dell'ideazione di tale sistema (da parte degli americani Diffie ed Helmann intorno al 1978), tutta la crittografia era basata (da millenni!) sulla sostanziale *unicità* della chiave di conversione dei caratteri alfanumerici perché basta leggere quella da usare per la criptazione (o «cifratura» che dir si voglia) in senso contrario per conoscere quella da usare per decriptare. Così, ad es., se nel codice di criptazione è stabilito che la lettera «A» di ogni parola di un testo va, trasformata nella lettera «Z», potrò servirmi di tale codice non solo per criptare, ma anche per decriptare: mi basterà leggere, al po-

sto della «Z», la «A»: in tal senso questo tipo di codice può ritenersi «*anfidromo*» (perché consente di correre dalla «A» alla «Z» e dalla «Z» alla «A») e le due chiavi («A» e «Z») si dicono *simmetriche* perché dall'una si può costantemente *risalire* all'altra. Anfidromia e simmetricità che risultano ancora più accentuate se, anziché redigere un codice dove per ogni segno alfanumerico sia stabilito il suo corrispondente criptico, si stabilisse, come fece Giulio Cesare per cifrare gli ordini da inviare ai suoi legionari sparsi per tutta la Gallia senza timore che i nemici potessero intercettarli e decifrare il significato, una formula costante (potremmo dire informaticamente un algoritmo) di conversione: ad es. che ogni lettera dell'alfabeto dovesse sempre intendersi sostituita dalla terza ad essa successiva secondo l'ordine alfabetico (quindi, ad es., la «D» al posto della «A», la «G» al posto della «D» etc.). Sistemi entrambi molto poco sicuri perché, se molti sono i possibili destinatari dei messaggi da far pervenire in tanti luoghi lontani e diversi, occorrerà fornire ogni possibile destinatario di una copia del codice (anfidromo) di conversione o far sapere ad ognuno di essi l'algoritmo unico da applicare per decriptare. Ma è evidente che, in tal modo, sarà relativamente facile che – o prima o poi – una copia del codice cada nelle mani dell'avversario o che egli venga a conoscere l'algoritmo, e che conseguentemente il sistema crittografico sia completamente vanificato e – peggio ancora – senza che chi su di esso fa affidamento si accorga neppure di tale vanificazione. La debolezza di ogni sistema crittografico a chiavi simmetriche (o «anfidrome» che dir si vogliano) non viene affatto meno se la trasmissione dei messaggi avviene telematicamente a mezzo del computer. In tal caso, trattandosi di comunicazioni a distanza tra soggetti che non si vedono tra loro (salvo il caso della videoconferenza), diventa sempre indispensabile (anche quando non vi siano particolari esigenze di segretezza) far riconoscere ad uno dei due (o più) comunicanti chi sia l'altro per la sicura imputabilità del messaggio ricevuto e per garantirne la fedeltà del testo.

A tal fine è stata ideata la «*password*», cioè una combinazione convenzionale di BIT corrispondente a determinati numeri (da 0 a 9) o a determinate parole (più facili da ricordarsi rispetto ai numeri), la cui esatta digitazione sulla tastiera del computer è condizione preliminare e indispensabile per accedere e consultare gli archivi di un sistema informatico e per eseguire nel suo ambito determinate operazioni riferibili a determinate persone. La password, quindi, serve anche a costituire un mezzo di riconoscimento personale dell'operatore

(tantoché, quando è costituita da un numero, esso viene chiamato «*personal identification number*» o, più brevemente, «P.I.N.») nonché della sua legittimazione sia a conoscere e a mutare i dati registrati nelle memorie del computer (c.d. abilitazione al «data-entry»), sia a dare ad esso ordini particolari per ottenere un certo output. La funzione della «password» è, quindi, quella di una chiave di sicurezza: non più metallica o di plastica (spesso a guisa di tesserino chiamato «badge»), ma, in conformità di una tendenza generale dell'informatica a smaterializzare gli oggetti tradizionali e a sostituirli con corrispondenti rappresentazioni del pensiero, costituita da semplici parole.

I vantaggi della password rispetto alle chiavi tradizionali sono molteplici[382], ma ha un «tallone d'Achille» relativamente facile a vulnerarsi: la perdita del segreto concernente la sua conoscenza. Perdita che l'utente non può non temere innanzitutto perché *egli non è il solo a conoscere la password*: essa, infatti, è certamente conosciuta o conoscibile, per la logica stessa del sistema che realizza, da chi tale sistema ha predisposto, se è persona diversa dall'utente, come nel caso in cui da un terminale periferico il cliente di una banca ordini un determinato movimento sul suo conto corrente. Egli, per farsi riconoscere dal sistema informatico e compiere l'operazione desiderata, deve preliminarmente usare una password (– per le carte di credito o di pagamento oggi solitamente un P.I.N. –), ma ciò implica necessariamente che, presso il centro elettronico della banca, vi sia una lista di tutti i P.I.N. previsti dal sistema e, a fianco di ciascuno di essi, il nome del titolare del conto corrente sul quale l'operazione ordinata deve essere eseguita. Se, per una qualsiasi ragione, occhi indiscreti si posano su tale lista, il segreto della password svanisce senza che l'interessato neppure se ne accorga. E non è neppure da escludersi che sia la stessa banca a commettere un errore nella redazione o consultazione di tale lista.

L'esistenza di questa lista di riscontro delle password costituisce una sorta di pericoloso codice crittografico a chiavi *simmetriche* (*anfidrome*) delle quali si è già detto per porne in evidenza la scarsa affidabilità, dacché le conoscenze necessarie e sufficienti sia per criptare che per decriptare sono sempre *condivise* quanto meno da due

[382] Vedi per la loro elencazione il § 216 del libro citato nella prefazione.

soggetti diversi e molto spesso lontani e che non si conoscono di persona: il mittente e il destinatario del messaggio.

227. *La superiorità dei sistemi a chiavi asimmetriche.* – È solo a questo punto che, dal confronto del sistema di crittografia a chiavi *simmetriche* con quello a chiavi *asimmetriche*, emerge l'assoluta superiorità di quest'ultimo per quanto concerne la sua affidabilità. Solo in quest'ultimo, infatti, l'autore del messaggio è *l'unico* soggetto che conosce il segreto del codice di conversione: cioè della chiave necessaria per criptare e che, proprio in riferimento a tale esclusività, il legislatore chiama «chiave privata»: *nessun altro* la conosce o, semplicemente, la conserva in deposito per essergli stata consegnata sia pure in plico chiuso. Al terzo fidefaciente e certificatore di cui si è dianzi accennato e che deve entrare in scena perché il sistema funzioni, dovrà, infatti, essere consegnata dall'autore del messaggio solo la sua *chiave pubblica*, quella, cioè, necessaria sì per decriptarlo ma di cui – come è stato già spiegato – non si può risalire a quella «privata» che, quindi, rimane veramente *segreta*. La legge (art. 28, comma 1, lett.g del D.P.R. 445/2000) proibisce, addirittura, che la chiave privata sia depositata (sia pure in plico sigillato) presso il certificatore fidefaciente. La superiorità della firma digitale rispetto alla password o al P.I.N. sta, quindi, nell'esclusività assoluta del segreto del codice per il fatto di non dover essere condiviso con nessuno[383], e quindi per il fatto che *non* esistono liste di riscontro dell'unica chiave segreta (o codici di corrispondenza che dir si vogliano). Da tutto ciò si traggono tre conseguenze:

- la prima è che, se l'autore dei messaggi da criptare, riuscirà a mantenere il segreto circa la sua «chiave privata» prendendo a tal fine tutte le precauzioni possibili e immaginabili in base al c.d. «stato dell'arte», nessuno riuscirà a spedire messaggi che falsamente gli siano imputabili e che egli non possa ripudiare;
- la seconda conseguenza è che egli sarà ritenuto il solo responsabile dell'omessa o imperfetta protezione del segreto, con tutte le conseguenze che da tale esclusiva responsabilità possono derivare;

[383] Caratteristica questa che il legislatore nell'art. 2 del d. lg. n. 10 del 2002 (lettera «g») esprime così: «univoca identificazione creata con *mezzi sui quali il firmatario può conservare un controllo esclusivo*».

- la terza conseguenza è che, alla firma digitale sono equiparabili, per grado di affidabilità, tutti quei sistemi di riconoscimento dell'identità personale che, pur non basandosi sulla duplicità di chiavi asimmetriche, riescono nel loro intento senza che esista alcuna lista di riscontro dei codici segreti e, quindi, quando essi siano conosciuti *esclusivamente* da un solo soggetto.

228. *Firma digitale e firma elettronica avanzata: la ricomprensione della prima nella seconda.* – Questa è la ragione per la quale nel d.lgvo n.10 del 2002 si distingue, in conformità della direttiva europea 1999/93/CE, la *firma digitale* dalla *firma elettronica avanzata* e si attribuiscono ad entrambe lo stesso valore: perché la caratteristica fondamentale della firma digitale e dell'importanza riconosciutale sta nell'*esclusività del segreto della chiave* (o «codice» che dir si voglia) di criptazione nel senso che tale segreto non è condiviso con nessuno *e perché la medesima caratteristica può essere realizzata, con l'ausilio dell'elettronica, anche con sistemi diversi da quello che va sotto il nome di firma digitale.*

Il più importante di essi, *alternativo* rispetto alla firma digitale[384], è quello basato sulla c.d. *chiave biometrica* che alla lettera g dell'art. 1 del D.P.R. n. 513 del 1997 è così definita:

«la sequenza dei codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente»: in altri termini potremmo dire su determinati *dati somatici* quali, ad esempio, l'impronta del dito, il disegno vascolare della retina dell'occhio, la tonalità delle corde vocali, ovviamente anche in combinazione tra loro, sicché, anche quando ciascuno di essi possa essere confondibile con quelle possedute da più persone, il fatto di trovarsi combinati insieme in una stessa persona in un determinato rapporto costituisca una sorta di *targa di riconoscimento* sicuramente esclusiva della sua identità. Ovunque questa targa sia registrata, per conoscere la persona cui si riferisca, sarà necessario e sufficiente metterne a confronto i dati con quelli rinvenibili nel suo stesso corpo, sicché esso sarà identificato nella sua fisicità per effetto semplicemente della loro corrispondenza e *senza neppure ricorrere al riscontro del nome della per-*

[384] Ma eventualmente anche aggiuntivo, come si spiegherà in seguito.

sona in quanto non raramente ciò che interessa è individuare il *corpo* di una persona, quale che sia il nome attribuitole. In tal modo, la chiave per effettuare il confronto e giungere al riconoscimento del corpo è costituita dal corpo stesso della persona: solo essa ne è ovviamente depositaria e solo essa decide quando metterlo a disposizione per il confronto, quindi, per il riscontro della sua identità: in tal senso è una chiave più che privata. La sicurezza del sistema è, da questo punto di vista, pari a quella garantita dalla firma digitale: *anzi superiore* perché, mentre la chiave privata, necessaria per realizzare detta firma, può essere «perduta» dal suo titolare (nel doppio senso sia della dimenticanza dei codici di conversione criptografica, sia di violazione del loro segreto da parte di estranei), invece la chiave privata, «*naturaliter*» iscritta nel corpo di una persona viene sempre necessariamente portata con sé e non può essere conosciuta da chi non abbia il potere di sottoporne il corpo ad un esame. Il sistema di riconoscimento, invero, può prevedere che, per funzionare, sia indispensabile che, avanti ad un computer, si presenti per il confronto una persona in carne ed ossa, sicché, anche ove fossero preconosciuti i dati delle targhe biometriche dei soggetti da sottoporre ad esame, sarebbe pressoché impossibile riprodurli e ricercarli nel corpo della persona con cui il riscontro andasse fatto.

Quanto sovraesposto in riferimento alle chiavi biometriche serve qui solo per chiarire che il fattore di maggior sicurezza della firma digitale (e cioè il fatto che una delle due chiavi necessarie per far funzionare il sistema possa essere conosciuta solo da un determinato soggetto) può essere realizzato anche con sistemi diversi da quello della firma digitale ideato da Diffie ed Helmann; sicché esso *non può oggi essere considerato l'unico possibile per conseguire il massimo di affidabilità sul piano legale.* Se il legislatore si fosse pronunciato a favore di una siffatta esclusività, avrebbe non solo commesso un arbitrio nella scelta del mezzo tecnico da preferire rispetto allo scopo da conseguire, ma anche negato, contro l'esperienza più comune, che, essendo oggi incessante il progresso scientifico e tecnologico, si può seriamente ritenere che quanto oggi non sia ancora sfruttabile sul piano pratico ma sia già teoricamente intravedibile sarà, o prima o poi, realizzato a beneficio di tutti, sicché sarebbe inammissibile bloccare un siffatto sviluppo sul rilievo che i traguardi già raggiunti non siano né eguagliabili, né superabili in futuro.

Saggiamente, dunque, il legislatore europeo ha previsto un sistema computerizzato di autenticazione degli scritti sostitutivo della

sottoscrizione autografa più largo di quello realizzato con la firma digitale nel senso che, *fermo restando quest'ultimo sistema in tutti i suoi dettagli già normativamente precisati*, esso possa essere affiancato, (in alternativa, ma , eventualmente anche in aggiunta come più avanti si chiarirà) da altri sistemi di pari efficacia giuridica perché di pari affidabilità tecnica.

Tenuto conto che il significato del termine «elettronica» è più ampio di quello attribuibile ad «informatica» in quanto i segnali elettronici possono essere tanto «digitali» (o «numerici» che dir si voglia perché costituiti dai numeri 0 ovvero 1, cioè dai BIT) quanto «analogici» (cioè misurabili solo per analogia con altri fenomeni non elettronici)[385], si spiega anche perché il legislatore del 2002 abbia voluto chiamare «*firma elettronica*» ogni sistema che, valendosi comunque dell'elettronica, consenta, sia pure con diverso grado di affidabilità, l'imputabilità dei messaggi telematici e «*firma elettronica avanzata*» la firma realizzata attraverso una procedura informatica che garantisca la connessione univoca al firmatario e la sua univoca identificazione, «*creata con mezzi sui quali il firmatario può conservare un controllo esclusivo*» e «collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati».

Conseguentemente la *firma digitale*, già istituita e disciplinata dal legislatore italiano nel 1997, viene ad essere *non* già sostituita dalla firma elettronica avanzata, *ma ricompresa* in quest'ultima categoria perché – come già in precedenza spiegato – realizzata con una chiave (quale, appunto, quella «*privata*») sulla quale il firmatario – cioè l'autore del messaggio – *conserva un controllo esclusivo* e collegato ai dati ai quali si riferisce (cioè al testo del documento informatico) in modo da impedirne qualsiasi alterazione.

Ma tale ricomprensione – come già si è accennato – non impedisce che possano essere ideati altri sistemi che consentano egualmente la sicura imputabilità dei documenti informatici, quali già si intravede potrebbero essere quelli basati sulle chiavi biometriche: non resterebbe che da studiare al riguardo come legare al sicuro riconoscimento dell'identità della persona l'imputabilità e l'intangibilità dei messaggi.

[385] Sulla differenza di significato tra i termini «elettronico» e «informatico» e sul loro rapporto raffigurabile come cerchi concentrici (più ampio quello elettronico e più ristretto quello informatico) vedi i §§ 2 e 3 del libro citato nella prefazione.

229. *La firma elettronica avanzata nel quadro dell'automazione sostanziale. I vantaggi che la firma autografa non soddisfaceva. In particolare: la segretazione dei messaggi.* – Essenziale – secondo il legislatore – è che si tratti di un sistema elettronico «*avanzato*», cioè progredito, sofisticato o, come più esaurientemente si sarebbe potuto dire, in grado di produrre un «*valore aggiunto*» rispetto a quello conseguibile per il semplice fatto di servirsi di un computer o, comunque, di mezzi elettronici. È, infatti, da tener presente che l'automazione può essere realizzata in due modi diversi: o facendo fare al computer le stesse operazioni che in precedenza si svolgevano a mano conseguendo, quindi, lo stesso risultato finale sia pure molto più comodamente e velocemente *ovvero* ideando un «modus operandi» totalmente nuovo e realizzabile solo in considerazione delle capacità elaborative e di memoria che il computer ha in misura enormemente maggiore rispetto a quelle «umane» in grado di conseguire un risultato finale molto più appagante rispetto a quello conseguibile senza l'uso del computer, non solo perché ottenuto più velocemente e più economicamente, ma, innanzitutto, perché raggiunge ulteriori e nuovi obbiettivi rispetto al passato che soddisfano esigenze che prima rimanevano insoddisfatte o soddisfatte in minor misura e talvolta neppure manifestate proprio perché si era convinti che non fossero soddisfacibili. Nel primo caso si deve qualificare *l'automazione come puramente formale*; nel secondo caso, invece, come *sostanziale*, perché solo in quest'ultimo si realizza un autentico progresso al di là delle forme e dei mezzi con cui un determinato risultato si ottiene.

La dimostrazione più evidente della differenza tra automazione puramente formale e automazione, invece, sostanziale si coglie proprio nella prospettazione dei modi possibili per sostituire la firma autografa nei messaggi telematici e tutelarne la riservatezza e, al tempo stesso, garantirne l'integrità del testo.

Per conseguire i primi due obiettivi si ricorreva – in era preinformatica – alla crittografia a chiavi simmetriche (cioè all'uso di codici anfidromi nel senso in precedenza spiegato), peraltro solo in casi eccezionali (per esigenze diplomatiche o militari) dato lo straordinario dispendio di tempo e di pazienza occorrente per trovare – sfogliando il codice – per ogni segno alfanumerico, il suo corrispondente criptografico. Col computer tale operazione di conversione è eseguibile in un battibaleno e senza alcuna fatica, ma, se il «modus operandi» della conversione fosse rimasto quello precedente (cioè quello a chiavi *simmetriche*), anche l'affidabilità del sistema sarebbe rimasta

al livello precedente: cioè scarsa, non essendo affatto improbabile (per le ragioni già esposte) che il codice o la formula di conversione venisse a conoscenza di persone non legittimate ad acquisirla.

Provvidenzialmente – in questo come in altri casi – si capì che, potendosi sfruttare le enormi e nuove potenzialità del computer, si poteva adottare, invece, *non solo uno strumento diverso, ma anche un metodo diverso* (quello appunto basato sulle chiavi *asimmetriche*) per effetto del quale il grado di affidabilità del sistema cresce enormemente perché una sola persona è a conoscenza della chiave per criptare (ed è, quindi, depositaria del suo segreto) anche quando migliaia e migliaia siano i possibili destinatari dei messaggi, in quanto dalla chiave di decriptazione (quantunque addirittura pubblica) non è dato mai risalire a quella (segretissima) necessaria per criptare.

In tal modo rimane soddisfatta anche l'esigenza di garantire *l'integrità* del testo trasmesso, esigenza che in era preinformatica rimaneva insoddisfatta proprio perché non vi era la possibilità tecnica di soddisfarla. Si ricorreva sì al sistema delle «postille» (sul presupposto che dovessero considerarsi efficaci solo le correzioni o integrazioni che apparivano apportate al testo originario convalidate «*post scriptum*» da apposita sottoscrizione autografa, ma anche in relazione a dette postille rimaneva pur sempre il sospetto di una loro alterazione successiva alla sottoscrizione di convalida.

E parimenti soddisfacibile col nuovo sistema delle chiavi asimmetriche è pure l'esigenza, talora avvertita, di tutelare il *segreto della comunicazione* impedendo ad estranei di intercettarla e di prenderne conoscenza[386]. Al riguardo, anzi, non si può fare a meno di notare che, qualora non si disponga di un computer, tale esigenza è soddisfacibile, per quanto riguarda i messaggi scritti, solo chiudendoli in una busta sigillata. Ma quest'ultima può sempre essere facilmente aperta anche da chi non sia legittimato a farlo, mentre, invece, il sistema di chiavi asimmetriche, utilizzabile anche per proteggere la segretezza dei messaggi teletrasmessi non è praticamente neutralizzabile. Il che induce a riflettere su una grande verità di principio e, cioè, sul fatto che le nuove tecnologie possano servire a rendere materialmente impossibile ciò che, prima, invece, materialmente era ben possibile anche se (giuridicamente) *illecito* (e, quindi, sanzionabile in via

[386] Questo effetto si ottiene mediante una doppia criptazione del messaggio: una prima con la propria chiave privata e una seconda con la chiave pubblica del destinatario (vedi il paragrafo 30 del libro citato nella prefazione).

civile o penale) e, conseguentemente, sulla opportunità di indirizzare il diritto sempre più ad adottare i nuovi mezzi tecnologici in grado di produrre tale effetto, essendo un grande principio di autentica civiltà giuridica quello secondo cui *prevenire*, pur rinunciando all'applicazione di sanzioni, sia cento volte preferibile che reprimere mediante condanne.

230. *La firma elettronica «debole».* – Tornando all'uso dell'elettronica per sostituire la firma autografa, devesi distinguere – in analogia con la distinzione poco innanzi delineata tra automazione puramente formale e automazione, invece, sostanziale – una *firma elettronica semplice* (o *debole*, che dir si voglia, quale quella che si realizza quando per crittografare o, comunque, per rendere imputabile uno scritto si usa lo stesso sistema usato in era preinformatica e, cioè, un codice anfidromo perché a chiavi simmetriche, con la conseguenza che certamente più di uno sono i soggetti a conoscenza della chiave di criptazione) e una *firma elettronica avanzata* (o *forte* che dir si voglia), quale quella che si realizza quando, invece, si usa il sistema nuovissimo (che solo l'uso del computer ha reso concepibile) delle chiavi asimmetriche o ad esso simile che non consente a nessuno (all'infuori, ovviamente, dell'autore del messaggio) di conoscere e disporre della chiave privata di criptazione. Firme elettroniche *semplici* (o *deboli* che dir si voglia) sono, ad esempio, come è stato già detto, le *password* e i P.I.N. Il legislatore non qualifica espressamente tali firme come *semplici o deboli* limitandosi a chiamarle «elettroniche», ma le suddette ulteriori aggettivazioni appaiono opportune perché costituiscono il naturale contrapposto logico dell'espressione «firma elettronica avanzata» che il legislatore, invece, espressamente usa. In particolare, appare opportuna la qualificazione di «debole» da attribuire a password e/o a P.I.N. non solo per la loro segretezza sempre molto relativa, ma anche perché – qualora essi siano costituiti da pochi caratteri alfabetici e/o numerici – possono essere oggi «scoperti» in pochi minuti mediante l'uso di computers, ancorché solo di media potenza, in grado di introdurre – grazie ad un particolare software –, nel «driver» del computer da violare, milioni e milioni di ipotesi di password e/o di P.I.N. diversi uno dopo l'altro in vertiginosa successione e, quindi, fino a trovare euristicamente la corrispondente a quella che si sarebbe dovuta conoscere preventivamente per accedere a un determinato sistema informatico e farlo funzionare.

231. *La funzione del certificatore (terzo fidefaciente) nel sistema della firma digitale.* – Postoché le firme elettroniche avanzate, quali sono le firme digitali, sono basate sull'uso di due chiavi diverse, di una delle quali il firmatario –come dice la legge- «*conserva il controllo esclusivo*» nel senso che egli solo la conosce e ne dispone, da ciò discendono due conseguenze, ineluttabili sul piano logico-funzionale e come tali previste dal legislatore.

Innanzitutto è necessario, infatti, che l'altra chiave sia conoscibile da tutti i possibili destinatari del messaggio (cioè da parte del pubblico) mediante interpello di un terzo fidefaciente (presso cui il titolare l'abbia preventivamente depositata) e che tale fidefaciente assicuri, rilasciando in proposito apposito *certificato* a chiunque glielo richieda, che la persona indicatagli è titolare di una certa chiave (pubblica) che in tal modo viene fatta conoscere per poterla usare come chiave di decriptazione, sicché quando la decriptazione riesce, si ha la prova oggettiva che il messaggio ricevuto proviene dal titolare della chiave comunicatagli dal certificatore. La serietà del *terzo certificatore* è quindi essenziale. Si comprende, così, la cura che nel d.lgvo 23 Gennaio 2002 n. 10 (art. 2) e nel D.P.R. 7 aprile 2003 n. 137 (art. 1, lettere «v» e «z») si pone per distinguere, nel novero dei «certificatori» (definiti come «coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche») i «*certificatori qualificati e accreditati*» in Italia ovvero in altri Stati membri dell'Unione Europea ai sensi dell'art. 3, paragrafo 2 della direttiva 1999/93/CE e nel novero dei «certificati elettronici» (definiti come «gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi»), i «*certificati qualificati*» (art. 2, comma 1, lettera «e» del d.lgvo 23 gennaio 2002 n.10) conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva.

Come emerge dall'art. 11 del d.lgvo n.10/2002 e dall'art. 27 del D.P.R. 28.12.2000 n. 445 sono da considerarsi «*certificatori accreditati*» (capaci, quindi, di rilasciare i «certificati qualificati») i certificatori iscritti nell'elenco pubblico (consultabile in via telematica) tenuto e aggiornato dall'A.I.P.A. (Autorità per l'Informatica nella Pubblica Amministrazione) dotati dei seguenti requisiti:

a) forma di società per azioni a capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria se soggetti privati;

b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;
c) affidamento che, per competenza ed esperienza i responsabili tecnici del certificatore e il personale addetto alla attività di certificazione siano in grado di rispettare le norme del regolamento e le regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione dei documenti informatici, definite con decreto del Presidente del Consiglio dei Ministri sentita l'A.I.P.A. e il Garante per la protezione dei dati personali;
d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

Certificatori *accreditati* sono da considerarsi anche le P.A. che provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione e all'utilizzo delle chiavi pubbliche delle P.A. (art.29 D.P.R. 445/2000).

Premesso che l'attività dei certificatori stabiliti in Italia o in altro Stato della Comunità Europea è libera e non necessità di autorizzazione preventiva purché, però, possiedano i requisiti di onorabilità richiesti per lo svolgimento di attività bancarie come specificato nell'art. 28 del D.P.R. 445/2000, ogni certificatore è tenuto, tra l'altro, a:

1) *identificare con certezza la persona che fa richiesta della certificazione*, cioè di chi intenda utilizzare un sistema di chiavi asimmetriche e depositi, a tal fine, la propria chiave pubblica;
2) specificare, su richiesta dell'istante e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;
3) revocare o sospendere tempestivamente il certificato nel caso in cui il titolare denunzi la perdita del possesso della sua chiave privata o revochi la sua chiave pubblica o vi siano sospetti di abusi o di falsificazioni, dandone immediata pubblicazione;
4) non rendersi in nessun caso depositario delle chiavi private di alcuno (neppure dei titolari delle chiavi pubbliche certificate);
5) adottare le misure minime di sicurezza di cui all'art. 15, comma 2 della l 675/96 sul trattamento dei dati personali e in particolare, adottare adeguate misure contro la contraffazione dei certificati.

Il certificatore, che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile del danno causato a chi su di esso abbia fatto ragionevole affidamento. Il certificatore può anche indicare nel certificato che rilascia, i limiti del suo uso, ivi compreso il valore-limite dei negozi per i quali può esser usato (art. 28 bis).

Si tenga, al riguardo, presente che l'apposizione ad un documento informatico di una firma elettronica basata su certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione.

232. *Il «dispositivo di sicurezza» per la generazione della firma digitale e la «smart-card» che lo contiene.* – Altro cardine fondamentale per l'affidabilità di una firma digitale o di altro tipo di firma elettronica di sicurezza avanzata è che la firma sia generata mediante l'uso di uno *speciale dispositivo* corrispondente ai requisiti prescritti dall'allegato III della direttiva europea 1999/93 la cui applicazione sia controllata in base a uno schema nazionale per la valutazione e la certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri e affidata ad un organismo pubblico indicato nello schema predetto. Il D.P.R. 7 aprile 2003 n. 137 (art. 1, lettera «hh») definisce «*dispositivo per la creazione della firma* il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica» e «*dispositivo sicuro* per la creazione della firma l'apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'art. 10 del d.lgvo 23 gennaio 2002 n. 10».

Ciò vuol dire, in altri termini, che i criteri per la creazione delle chiavi asimmetriche (privata e pubblica della firma digitale) come pure di altri sistemi di firme elettroniche avanzate, e, quindi, gli algoritmi e le procedure necessarie per la loro applicazione non possono essere lasciati – per ovvie ragioni di pubblica affidabilità – alla discrezionalità di ciascun firmatario e alla fiducia che egli, nell'applicarli, e nel farne di volta in volta uso non commetta errori, ma devono essere programmate in un software immodificabile, autorizzato e controllato dall'Autorità, racchiuso in una *smart-card*, (normalmente costituita da una scheda di plastica contenente microcircuiti e chips e, quindi, un vero e proprio microcomputer), la cui introduzione nel computer del firmatario sia necessaria e sufficiente per generare, con criteri di casualità, una chiave segreta con cui criptare i messaggi, e una chiave pubblica correlata con cui decifrarli.

Tale «*smart-card*»non solo realizza quello *speciale dispositivo di sicurezza* che, come è stato già detto è il secondo presupposto di affidabilità della firma digitale (oltre quello della certificazione concernente la titolarità della chiave pubblica), ma serve a sollevare il firmatario dall'onere di ricordare e di applicare correttamente tutta la procedura necessaria per firmare digitalmente (e riprodotta, passo passo, nel libro citato nella prefazione) e, quindi, a renderla alla portata di tutti: basterà introdurre la «smart card» nel proprio computer e indicare il testo di un messaggio preventivamente registrato nelle sue memorie sottoforma di «file» e l'indicazione del suo destinatario perché la firma digitale possa considerarsi apposta a quel testo. A ben vedere – lo ricordiamo ancora una volta – *non è, quindi, una sottoscrizione*, ma *un'associazione di una specie di sigillo a un determinato testo.*

233. *La «firma qualificata» (o sicura che dir si voglia).* – Il legislatore, negli artt. 6 (comma 3), 9 (comma 1) e 10 (commi 1 e 3) del d.lgvo. 23 gennaio 2002, n10, chiama tale *dispositivo di sicurezza* (necessario per generare, in maniera affidabile, le chiavi asimmetriche da attribuire al titolare della firma digitale) «*dispositivo per la creazione di una firma sicura*». Nel D.P.R. 7 aprile 2003 n. 137 (art. 1, lettere «ee» e «ii») l'aggettivo «sicuro» viene riferito al dispositivo avente certi requisiti e alla locuzione «firma sicura» viene sostituita quella di «firma elettronica qualificata».

Tali variazioni terminologiche possono certamente disorientare, ma al di là di esse, sembra di poter ritenere che la «firma sicura» altro non sia che la «firma elettronica qualificata» e che quest'ultima, a sua volta, non sia altro che una *firma elettronica avanzata* (nozione nella quale rientra la firma digitale), avente, però, due requisiti in più: quello concernente il certificatore e quello concernente il dispositivo di sicurezza.

In altri termini, può dirsi che, perché si abbia una *firma elettronica qualificata* (alias: *sicura*) devono concorrere tre requisiti:

1) che la chiave per riconnettere un determinato nome *a una determinata persona sia posseduta e conosciuta* solo dal titolare (come nel sistema delle chiavi asimmetriche e delle chiavi biometriche come, invece, *non* avviene col sistema dei P.I.N. e delle password);
2) che le chiavi asimmetriche siano generate in maniera affidabile e, quindi, mediante un *dispositivo sicuro per la creazione della firma*;

3) che altrettanto affidabile sia il terzo certificatore della titolarità della chiave pubblica, (certificatore *qualificato* o *accreditato*) e che, quindi, egli emetta certificati *qualificati.*

Solo coesistendo tutte e tre queste condizioni una firma digitale può considerarsi *firma sicura* e per ciò stesso *qualificata*, nel senso che, in tal caso, è ragionevole presumere che una determinata persona abbia «firmato» un determinato testo.

234. *Il carattere personale e indisponibile della smart-card e del dispositivo che contiene.* – Perché tale ragionevolezza venga meno, e la querela di falso possa essere accolta occorre, immaginare queste tre ipotesi: che il firmatario sia stato costretto da altri a usare la «smart-card» contenente il dispositivo necessario per generare e usare la chiave segreta (vis atrox) o che gli sia stata sottratta (furto) senza che se ne sia neppure accorto o l'abbia smarrita o comunque non diligentemente custodita, sicché altri ne abbia fatto uso mettendo in atto, in sostanza, una sostituzione di persona. Casi, peraltro, poco probabili sia in considerazione del livello di professionalità e di cultura riscontrabile, almeno oggi, in chi vuol servirsi della firma digitale, sia perché l'uso della «smart-card» può, a sua volta, essere protetto mediante l'uso di un P.I.N. o di una password, sufficienti ad evitare che chiunque venga in possesso di detta smart-card possa, «sic et simpliciter», utilizzarla indebitamente. Al di fuori di tali casi la querela di falso non deve essere ritenuta ammissibile dovendo rimanere sempre strettamente attinente alla provenienza del documento nella sua materialità di testo scritto.

Diciamo «indebitamente» perché non può escludersi che il titolare di essa la consegni *volontariamente* ad altri perché apponga la firma digitale del titolare stesso sui documenti informatici. La legge non prevede tale caso, ma, da tutto l'insieme delle norme che riguardano la firma digitale, sembra doversi desumere che una *siffatta «delega» del potere di firmare non sia consentita*, trattandosi di un potere indisponibile per l'esigenza d'ordine pubblico che la firma sia ritenuta «erga omnes» propria di chi appare averla apposta: la stessa esigenza di tutela della fede pubblica che rende illecita e, quindi, nulla l'autorizzazione data ad altri di falsificare la propria firma autografa (cioè la firma dell'autorizzante). L'uso della «smart-card», contenente il dispositivo di sicurezza per firmare digitalmente, deve essere, quindi, considerato *strettamente personale* e assolutamente non cedibile, sicché chi contravvenisse a tale principio non sarà mai ammesso a con-

testare la veridicità della sua firma in quanto «*nemo auditur alligans turpitudinem suam*».

Sembra, invece, lecito che il titolare del dispositivo di firma e della smart card che lo incorpora lo inserisca permanentemente in un suo computer programmato per stipulare ciberneticamente (cioè in assensa del *dominus*) contratti in nome e per conto di lui anche se il contenuto del contratto non è da lui preventivamente conosciuto e consentito in tutte le sue precise determinazioni, potendo essere il frutto di una conbinazione imprevista degli IF dei softwares dei computers delle rispettive parti contraenti.

Di tali contratti cibernetici era stata messa in dubbio la validità, in quanto il loro contenuto, a differenza di quelli semplicemente telematici, può essere diverso, almeno in parte, da quello che il *dominus* prevedeva e quindi non fondato su una sua volontà precisa. Ora l'ostacolo può considerarsi superato, in quanto *l'uso automatico del dispositivo di firma digitale*, rendendo, non ripudiabile da parte del titolare di essa il contenuto del contratto, crea una situazione perfettamente analoga a quella in cui egli si rovi quando, per effetto della procura *ad negozia* conferita a un suo rappresentante, non possa ripudiare il contratto da quest'ultimo stipulato in suo nome e per suo conto. Può questa prospettiva legittimare la configurabilità di un vero e proprio *automa giuridico sul piano negoziale*?

235. *La firma digitale autenticata.* – Tutto quanto sopraesposto spiega anche perché, come già previsto nell'art. 16 del D.P.R. 10 Novembre 1997 n. 513 e confermato nell'art. 24 del D.P.R. 28 Dicembre 2000 n. 445, la *firma digitale può essere autenticata* e l'autenticazione consiste nell'attestazione da parte di un pubblico ufficiale (notaio o altro pubblico funzionario a ciò espressamente autorizzato) che «la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'art. 28, primo comma, n. 1 della l. 6 Febbraio 1913 n. 89».

In merito alla predetta autenticazione, di cui si parlerà ancora anche più avanti (vedi al § 240) due considerazioni si impongono subito[387].

La prima consiste nel rilevare che, nonostante l'adozione delle

[387] Sulla firma digitale autenticata v. anche il § 240. V. anche di G. Rognetta, *La firma digitale e il documento informatico*, Simone, 1999, il cap. 4, § 8.

procedure più sofisticate per garantire la fede pubblica in relazione alle firme, il problema preliminare e fondamentale rimane sempre (purtroppo!) quello di accertare l'identità del firmatario, cioè l'identità della persona (intesa come corrispondenza tra un corpo e un nome), problema che non è stato ancora soddisfacentemente risolto, quantunque già si intraveda il contributo che l'informatica può dare a risolverlo mediante un sistema di identificazione personale basato prevalentemente sulle c.d. «chiavi biometriche» delle quali si è parlato in precedenza.

La seconda considerazione riguarda quale senso possa attribuirsi all'obbligo che la legge impone al notaio (o a chi per lui) di accertare, in sede di autenticazione della firma digitale, anche «la validità della chiave utilizzata». È assolutamente da escludersi – perché contrario a tutto il sistema della firma digitale – che l'autenticante possa farsi comunicare la chiave segreta del firmatario o fare alcunché per ricostruirla operando una sorta di «reverse enginering» sulla «smart-card». La legge (art. 26 del D.P.R. 445/2000) prevede sì che la chiave privata possa essere depositata presso un notaio o altro pubblico depositario autorizzato, ma pur sempre *in forma segreta* e, quindi, come avviene per il testamento segreto consegnato al notaio, senza che questi – o altri – ne prendano cognizione.

La «validità della chiave segreta utilizzata» non potrà, pertanto essere accertata che mediante riscontro della conformità del dispositivo di sicurezza incorporato nella «smart-card», almeno da un punto di vista apparente, ai requisiti prescritti dalla legge (art. 10 d.lgvo 23 Gennaio 2002 n. 10) ed, eventualmente (a discrezione del notaio) anche mediante una *prova* di detta validità, consistente nel lanciare un messaggio con firma digitale e nel controllare poi se la persona indicata dal certificatore corrisponda a quella comparsa avanti al notaio e il testo decriptato con la chiave pubblica indicata nel certificato corrisponda esattamente al testo criptato con la chiave privata. Al riguardo deve tenersi presente che nel D.P.R. 7 aprile 2003 n. 137 (art. 1, lettera «mm») si prevede un *dispositivo di verifica* della firma elettronica definito così: «il programma informatico (software) adeguatamente configurato o l'apparato strumentale (hardware) usati per effettuare la verifica della firma elettronica».

236. *Il valore probatorio del documento informatico a seconda del tipo di «firma» di cui è munito.* – Tutto quanto fin qui detto in ordine al documento informatico e ai possibili modi di firmarlo ci

permette ora di capire agevolmente le norme dettate per disciplinarne il valore e l'efficacia sul piano giuridico, risolvendo le questioni sorte dal loro rapido succedersi e dalla incostante terminologia usata, in un primo momento (comma 2, art. 15 della l. 15 Marzo 1997 n. 59 c.d. legge Bassanini) ci si limitò a stabilire il principio che «Gli atti, dati e documenti firmati dalla P.A. e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge».

Posto questo principio fondamentale, con pedissequo regolamento emanato con il D.P.R. 10 Novembre 1997 n. 513 si stabilì, all'art. 4, che «il documento informatico, munito dei requisiti previsti dal presente regolamento, *soddisfa il requisito legale della forma scritta*», all'art. 5 che «il documento informatico, sottoscritto con la firma digitale...*ha efficacia di scrittura privata ai sensi dell'art. 2702 c.c.*», all'art. 10 che «l'apposizione della firma digitale al documento informatico, equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo. L'apposizione della firma digitale integra e sostituisce... l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere», all'art. 11 che «i contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale, sono validi e rilevanti a tutti gli effetti di legge», all'art. 16 che «si ha per riconosciuta ai sensi dell'art. 2703 c.c. la firma digitale la cui apposizione è autenticata da notaio o da altro pubblico ufficiale...».

Tale normativa, quantunque essenziale per la forza dirimente e innovativa dei principi posti, era però insufficiente a costituire un quadro esauriente del valore e dell'efficacia del documento informatico. Si ponevano, innanzitutto, due quesiti: il primo se, al di fuori della firma digitale, non vi fossero altri sistemi legali per l'attribuzione di una comunicazione telematica ad una persona e quale valore avesse, quindi, un documento informatico privo di firma digitale; il secondo come dovesse interpretarsi il riferimento fatto nell'art. 5 sopramenzionato alla scrittura privata di cui all'art. 2702 c.c. Quest'ultimo articolo, infatti, stabilisce sì che la scrittura privata si considera riconosciuta quando:

1) colui contro il quale la scrittura sia stata prodotta ne riconosca la sottoscrizione ovvero:
2) questa sia da considerarsi legalmente come riconosciuta in quanto:

a) la sottoscrizione sia stata autenticata da notaio o da altro pubblico ufficiale (art. 2703 c.c.)

oppure:

b) sussista la contumacia della parte contro cui la scrittura è prodotta (art.215 c.p.c.) oppure:
c) non vi sia stato disconoscimento formale e tempestivo (artt.li 214 e 215 c.p.c.) oppure:
d) sia risultato positivo l'esito del giudizio di verificazione dell'autenticità dell'autografia posta a confronto con altre sottoscrizioni autografe o, comunque, altri manoscritti della parte contestatrice.

Dovevano e *potevano* tali condizioni essere richieste anche per il documento informatico firmato digitalmente? Se, nella maggior parte dei casi, basta vedere una firma tradizionale per sospettare se sia la propria ovvero se sia stata da altri falsificata e, quindi, per riconoscerla, tale controllo visivo – chiaramente posto a base dell'art. 2702 c.c. e delle altre norme cui esso rinvia – certamente non può essere effettuato in relazione ad una firma digitale. Ma, d'altra parte, ritenere che l'art. 2702 c.c. potesse applicarsi al documento informatico senza le condizioni sopramenzionate, avrebbe significato non già equiparare il valore probatorio del documento informatico a quello cartaceo, ma addirittura, attribuirgli un valore superiore, in aperto contrasto con il conclamato proposito legislativo di stabilire una equivalenza tra le due forme di documento, non già una superiorità dell'uno rispetto all'altro.

Per dirimere tutte queste incertezze e regolare più completamente e persuasivamente tutta la materia sono intervenuti, in una successione temporale e con collegamenti (espliciti o impliciti) certamente tutt'altro che encomiabili, il D.P.R. 28 Dicembre 2000 n. 445, il decreto legislativo 23 Gennaio 2000 n. 10 in attuazione della direttiva dell'Unione Europea 1999/93/CE relativa ad un «quadro unitario per le firme elettroniche» e, infine, il D.P.R. 7 aprile 2003 n. 137 («regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'art. 13 del d.lgvo 23 gennaio 2002 n. 10»). Coordinando come più ragionevolmente sembra possibile – anche se con un certo sforzo – tutte queste norme, appare delineabile, per quanto concerne le varie specie di documenti informatici e di firme elettroniche (che comprendono anche la firma digitale) e del conseguente valore probatorio, lo schema di cui appresso:

a) DOCUMENTO INFORMATICO SPROVVISTO DI QUALSIASI FIRMA ELETTRONICA che ne attesti la provenienza: semplice rappresentazione in BIT (cioè informatica) di qualsiasi scritto, suono o immagine. Esso è pur sempre un documento anche dal punto di vista giuridico e, come tale, *ha l'efficacia prevista dall'art. 2712 per le riproduzioni meccaniche dei fatti o delle cose rappresentate* (come se si trattasse di fotografia o di film o di registrazione fonografica): «fatti o cose di cui fa piena prova se colui contro il quale il documento è prodotto non ne disconosce la conformità ai fatti o alle cose medesime». In tal senso deve interpretarsi il 1° comma dell'art. 6 del d.lgvo 23 Gennaio 2002 n.10 che così recita: «il documento informatico ha l'efficacia probatoria prevista dall'art. 2712 c.c., riguardo ai fatti e alle cose rappresentate».

Tenuto conto che, nelle memorie di un computer, uno scritto (con relativa sottoscrizione autografa) può essere memorizzato, volendo, anche *per identità di immagine* e cioè esattamente come una *fotografia* dello scritto medesimo (vedi, in proposito, il § 15 del libro citato nella prefazione), si pone il problema del valore probatorio di siffatta fotografia digitale una volta riprodotta in «output». Se lo scritto fotografato è un contratto o altro negozio giuridico, possono i medesimi ritenersi provati ai sensi del combinato disposto del citato art. 6 (comma 1) con l'art. 2712 del c.c.? Al riguardo occorre distinguere se il negozio sia dedotto come fonte diretta di diritti od obblighi reciproci fra le parti contraenti ovvero se esso sia dedotto come *semplice fatto storico*, come può avvenire, ad esempio, o quando sia dedotto da un terzo ovvero anche tra le parti, quando, incontestata l'esistenza di un contratto e il tenore delle sue clausole, lo scritto, di cui si produce la fotografia, serva soltanto per la loro interpretazione[388]. In tali casi, come non si applicano le limitazioni poste dalla legge all'ammissibilità delle prove testimoniali, così non vi dovrebbero essere ostacoli ad ammettere, purché semplicemente come prova di un fatto storico, anche l'immagine computerizzata di uno scritto, riprodotto, anche per quanto riguarda l'autografia della sottoscrizione, come se fosse stato fotografato (come ben può avvenire quando si disponga di un computer dotato di una stampante a getto d'inchiostro).

A questo proposito è da ricordare che, per le ragioni già spiegate in precedenza, alla firma autografa del documento informatico

[388] Cfr. Cass. Civ. sent. n. 659/99 e n. 5662/92 e 1838/90.

non può attribuirsi –per difetto di affidabilità dovuta alla scorporablità dal supporto- alcun valore legale per quanto concerne la *formazione* di un contratto (o di altro negozio giuridico) che si sostenga avvenuta con la compilazione di quel documento informatico (salvo che, come già detto, tale formazione non sia addotta come puro fatto storico). A ben diversa conclusione riteniamo, invece, possa pervenirsi se si sostenga che il negozio è stato formato (e quindi originariamente posto in essere) *con un documento cartaceo munito di sottoscrizione autografa* e che il documento informatico esibito – per le caratteristiche del software che lo ha generato – non sia altro che la *copia fotografica digitale* riproducente, per identità di immagine, il documento cartaceo anzidetto. In tal caso ci sembra applicabile non l'art. 2712 c.c., bensì l'art. 2719 stesso codice il quale – con maggiore aderenza alla fattispecie – così recita «Le copie fotografiche di scritture hanno la stessa efficacia delle autentiche se la loro conformità con l'originale è attestata da pubblico ufficiale competente ovvero non è espressamente disconosciuta». È ben vero che il d.lgvo n.10/2000 cita soltanto l'art. 2712 e non anche il 2719, tuttavia non ci sembra che tale omissione ne impedisca l'applicazione nella fattispecie, in quanto, con l'evocazione dell'art. 2712, il legislatore sembra essersi preoccupato soltanto di escludere che la fotografia digitale di un documento recante firma autografa possa servire di per se stesso a *formare* un negozio che debba essere redatto per iscritto «*ad subastantiam*» o anche semplicemente «*ad probationem*», senza prendere affatto in considerazione il ben diverso caso della *fotografia digitale di un preesistente originale* costituito da un documento *cartaceo* e senza, quindi, che possa farsi applicazione del noto principio ermeneutico secondo cui «*inclusio unius, esclusio alterius*».

D'altra parte, che la riproduzione *per identità di immagine* di un documento (la stessa cui si riferisce l'art. 2220 c.c. così come modificato dalla l. 8 agosto 1994 n.489 che convertì l'art. 7 bis del d.l. 10 giugno 1994 n.357 in tema di conservazione di scritture contabili) possa considerarsi alla stregua di una «*copia fotografica*» cui si riferisce l'art. 2719 c.c., sembra ben sostenibile, sia perché alla copia fotografica è stata sempre assimilata la copia fotostatica o xerografica che dir si voglia (in tal senso giurisprudenza assolutamente costante) pur trattandosi di riproduzioni ben diverse per il modo[389] con cui

[389] Per la differenza tecnica tra fotografia e xerografia vedi la nota n. 14 del paragrafo 15 del libro citato nella prefazione.

vengono realizzate dandosi così prevalenza ermeneutica all'analogia del risultato finale piuttosto che alle sottostanti differenze tecniche, sia in considerazione del fatto, ormai notorio e scientificamente incontrovertibile, che una immagine può essere riprodotta perfettamente anche mediante una serie di BIT (vedi al riguardo il § 15 del libro citato nella prefazione). Né può addursi in contrario, che, essendo i BIT elaborabili a piacere a seconda del software del computer, l'immagine da quest'ultimo riprodotta non darebbe quell'affidabilità (sotto il profilo della fedeltà alla cosa riprodotta) che potrebbe dare solo una copia fotografica o fotostatica. È noto, infatti, che alterazioni dell'immagine sono possibili anche nelle fotografie mediante «fotomontaggi» o mediante riproduzione di immagini incomplete (v. al riguardo Cass. Sent. n. 1772/77).

Da tutte le suesposte considerazioni deriva che chi si veda recapitare *da un computer* uno scritto con firma manoscritta autografa *sedicente copia di un contratto* o altra dichiarazione giuridicamente impegnativa, deve immediatamente (a processo già instaurato sin dalla prima udienza o dalla prima difesa successiva ai sensi degli art.li 214 e 215 c.p.c.)[390], disconoscere espressamente la conformità di tale copia all'originale, a meno che – più radicalmente – non neghi addirittura trattarsi di copia *per inesistenza* di un qualsiasi originale cartaceo. Se tale inesistenza rimarrà accertata, il documento informatico esibito non avrà più alcun valore. Se, al contrario, ne rimarrà accertata l'esistenza, il documento informatico dovrà esserne considerato copia fotografica (digitale) *conforme* indiscutibilmente all'originale se, al riguardo di tale conformità, non sia stata sollevata tempestiva contestazione. Va comunque tenuto presente che, anche qualora tale contestazione vi sia stata, essa non impedirà che il giudice possa accertare la conformità all'originale *anche attraverso altri mezzi di prova, comprese le presunzioni*[391]. Sotto tale profilo infatti, la giurisprudenza della Corte di Cassazione è costante nell'affermare che il disconoscimento della conformità di una delle riproduzioni menzionate nell'art. 2712 c.c. ai fatti rappresentati *non* ha gli stessi effetti del disconoscimento previsto dall'art. 215, comma 2, c.p.c. della scrittura privata perché solo quest'ultimo – a differenza del primo – preclude l'utilizzazione della scrittura in mancanza di richiesta di verificazione e di esito positivo di questa.

[390] Applicabili, secondo la giurisprudenza assolutamente prevalente anche nel caso di cui all'art. 2719 c.c.: vedi in tal senso da ultimo Cass. sent. n.ro 4661 del 2 Aprile 2002.

[391] In tal senso Cass. 11445/2001, 12 maggio 2000 n. 6090 in tema di copie fotostatiche, 26 gennaio 2000 n. 866 e 5 febbraio 1996 n. 940 in tema di copie fotografiche, 22 dicembre 1997 n. 12949 in tema di tabulati informatici riepilogativi di retribuzioni, 8 luglio 1994 n. 6437 in tema di dischi cronotachigrafi, 10 settembre 1997 n. 8901 sugli oneri probatori dell'utente che contesti la corrispondenza al proprio traffico telefonico delle risultanze del misuratore di centrale).

b) DOCUMENTO INFORMATICO CON FIRMA ELETTRONICA DEBOLE (o «semplice» che dir si voglia: comunque nel senso di *NON* avanzata), cioè, come è stato già detto in precedenza, costituita da un insieme di BIT usati come strumento di autenticazione informatica del testo cui sono associati, a guisa di «chiave» *che, però, non è completamente sicura in quanto conosciuta (o conoscibile) anche da persone diverse dal firmatario (es.: password o P.I.N.).* Ai sensi del comma 2 dell'art. 6 del d.lgvo del 23 gennaio 2002 n. 10 un siffatto documento *«soddisfa il requisito legale della forma scritta»*. Non avendo il legislatore posto alcuna limitazione a tale enunciazione di carattere così generale, deve ritenersi soddisfatta la forma scritta anche quando essa sia richiesta *«ad probationem»*o *«ad substantiam»* (cioè a pena di nullità) per la validità e l'efficacia di un negozio giuridico. Soddisfa anche l'obbligo posto a carico dell'imprenditore dall'art. 2214 c.c. della tenuta dei libri obbligatori e dalle altre scritture contabili. Pertanto il «libro giornale», il «libro degli inventari» e ogni altra scrittura contabile richiesta dalla natura e dalle dimensioni dell'impresa potranno essere tenuti *fin dall'origine* (cioè dal loro nascere) sottoforma di BIT registrati nelle memorie di un computer, purché vi sia un qualche sistema, anche non completamente sicuro, di collegamento di tali dati alla persona dell'imprenditore.

Al riguardo della validità del documento informatico sottoscritto con firma elettronica *debole* l'art. 24 del D.P.R. 445/2000 (riprodotto nel comma 4 dell'art. 6 del d.lgvo n. 10/2002 precisa che: «Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura». Il che vuol dire, in sintesi, che una firma elettronica è giuridicamente rilevante e attribuisce al testo documentato valore di «scrit-

tura» anche se gli mancano i requisiti per essere considerata firma elettronica avanzata (come lo è la firma digitale) e, ancor più, «firma sicura» (o «qualificata»).

Tutti i documenti informatici sottoscritti con firma elettronica *debole* non hanno, però, un valore probatorio preciso e indiscutibile in quanto, come lo stesso comma 2 sopracitato dispone, «*sono liberamente valutabili*, tenuto conto delle loro caratteristiche oggettive di qualità e di sicurezza». Il giudice, quindi, – a cui in definitiva sarà rimessa tale valutazione – potrà al riguardo servirsi anche di presunzioni semplici che gli permettano di distinguere il grado di affidabilità che ad un sistema di password, di P.I.N. o di altri strumenti informatici simili può attribuirsi. Tali sistemi, infatti, – come diffusamente spiegato nel § 216 del libro citato nella prefazione – possono essere talmente semplicistici da non offrire alcuna garanzia di sicurezza (si pensi ad una password o ad un P.I.N. di pochi caratteri alfanumerici che oggi, proprio con l'ausilio di tecniche euristiche realizzabili con un computer programmato ad hoc anche se non di grande potenza, sono scopribili in pochi secondi come pure, al contrario, possono essere così sofisticati, mediante ricorso ai più complessi e fantasiosi algoritmi, da resistere anche alle sfide degli hackers più temibili).

Il documento munito di firma elettronica debole *non* possiede, quindi, l'efficacia probatoria tipica e indiscutibile della scrittura privata sottoscritta che, invece, ai sensi dell'art. 2702 c.c. «fa piena prova *fino a querela di falso* se riconosciuta o se deve essere legalmente considerata come riconosciuta».

Conseguentemente, il documento munito di firma elettronica *debole* può essere sempre impugnato liberamente da chiunque vi abbia interesse. Sotto questo aspetto, il documento «de quo» ha una minore efficacia probatoria del documento informatico non munito di alcuna firma elettronica che sia fatto valere come riproduzione meccanica dei fatti e delle cose rappresentate o come copia di uno scritto cartaceo che, come tale, non sia stata tempestivamente contestata. Tali riproduzioni infatti, fanno piena prova – ai sensi degli art.li 2712 e 2719 c.c. – dei fatti o delle cose predette.

c) DOCUMENTO INFORMATICO CON FIRMA DIGITALE O con altro tipo di FIRMA ELETTRONICA AVANZATA

- basata su un *certificato qualificato* e
- generata mediante un dispositivo per la creazione di una «firma sicura».

Concorrendo queste tre condizioni tale documento «fa *piena prova fino a querela di falso* della provenienza e delle dichiarazioni di chi l'ha sottoscritto» (art. 6, comma 3 del d.lgvo n. 10/2002): ha, cioè, lo stesso valore di una scrittura privata *riconosciuta*, sicché non è possibile disconoscerla ed è impugnabile solo con la querela di falso.

237. *Querela di falso e responsabilità del querelante.* – Ricorrendo tali condizioni e tenuto conto dell'effetto della loro convergenza come sopraesposto, può ben dirsi che la *firma digitale diventa una «firma sicura»* nel senso che merita quest'ultimo appellativo. Da ricordare, al riguardo, che la firma «sicura» viene chiamata nel D.P.R. 7 aprile 2003 n 137: «firma elettronica qualificata», ma tale nuova espressione non sembra cambiare il quadro della disciplina previgente in materia, sicché sarebbe stato meglio continuare a parlare di «firma sicura». Ciò non toglie, però, che, come è stato già detto, anche tale «firma *qualificata*» (o «*sicura*» che dir si voglia) debba essere *autenticata* da un notaio (o da altro pubblico ufficiale a ciò autorizzato) tutte le volte in cui la legge richieda un atto (cartaceo) con firma autografa autenticata (come, ad esempio, per ottenere la trascrizione di una compravendita immobiliare): e ciò perché, come per la firma autografa il notaio deve attestare che essa è stata vergata alla sua presenza dalla persona il cui corpo corrisponde al nome fatto palese dalla firma al fine di dirimere ogni eventuale dubbio sulla falsità di quest'ultima, così, per la stessa esigenza di certezza, è necessario che un pubblico ufficiale accerti che la smart-card (contenente il dispositivo di sicurezza per generare la firma digitale) venga usata a tal fine proprio dalla persona fisica che ne è titolare: quindi, non solo senza apparente costrizione, ma anche dirimendo il sospetto di alcuna *sostituzione di persona* o di alcuna irregolarità nell'uso del dispositivo di firma necessario.

Ovviamente anche un documento informatico con «firma digitale sicura» o «autenticata» potrà pur sempre essere impugnato con querela di falso (come, del resto, può esserlo lo stesso atto pubblico ai sensi dell'art. 2700 c.c.): quindi con lo stesso mezzo esperibile per impugnare un documento informatico con firma sicura *non* autenticata. Ma è appena il caso di rilevare che, nella prima ipotesi, sarà molto più difficile (che non nella seconda) provare che la «smart-card» non sia stata usata personalmente dal titolare[392].

[392] Sulla firma digitale autenticata vedi anche il § 238.

238. *La responsabilità eventuale del titolare della firma digitale in caso di accoglimento della querela di falso.* – Anche quando la querela di falso sia accolta e l'atto sia stato posto nel nulla, ben potrà il querelante vittorioso essere, ciononostante, condannato ai danni nei confronti di chi , senza sua colpa, abbia fatto affidamento sulla validità del documento informatico quando emerga che alla causazione del falso abbia concorso il querelante per aver omesso di custodire con la massima diligenza la smart-card contenente il dispositivo necessario per generare la firma digitale o, comunque, il segreto più assoluto relativo alla sua chiave privata. Il grado di diligenza nell'adempimento di un dovere, infatti, deve sempre essere commisurato alla gravità degli effetti che la sua violazione potenzialmente produce, sicché, nella specie, trattandosi di assicurare la buona fede dei contraenti, la fede pubblica in generale e lo sviluppo dell'economia collettiva, tutti beni di grandissimo valore, il titolare del dispositivo di firma dovrà prendere tutte le precauzioni che l'odierna tecnologia consente per impedire la violazione del segreto o effetti ad esso equivalenti: protezione, quindi, della «smart-card» con sofisticati sistemi di password o di P.I.N. o, ancora più efficacemente, con chiavi biometriche tali da impedire che della smart-card possa essere fatto uso da persona fisica diversa dal titolare.

239. *Conclusioni.* – Tutta la normativa sul documento informatico e sulla firma elettronica sin qui esaminata trova la sua giustificazione sia nelle esigenze del commercio elettronico (che non decollerà veramente fino a che, sul piano legale non si abbia la diffusa convinzione di poter fare affidamento su una «firma digitale sicura») e, quindi, della «new-economy», sia nella opportunità di snellire al massimo i rapporti tra privati e la Pubblica Amministrazione, sia, più in generale, nella constatazione che alla corrispondenza epistolare tradizionale e all'uso della posta va sostituendosi sempre più l'uso dell' «e-mail» per la fulmineità e quasi gratuità della trasmissione dei messaggi che consente. Perché tutte queste esigenze fossero soddisfatte e, in particolare, perché uno strumento più rapido, più in linea con i nuovi tempi, potesse apparire idoneo a sostituirsi al servizio postale (il quale, paradossalmente sembra incontrare non poche difficoltà, a recuperare quell'altissimo livello di funzionalità e di apprezzamento che un tempo aveva)[393] occorreva, infatti, certamente sostituire al-

[393] Ricordo che, negli anni 1950/1952, in Italia, due lettere-espresso, imbucate alle ore 20 del sabato, rispettivamente presso la buca postale delle stazioni ferroviarie di Roma e di Varese, giungevano a destinazione (l'una a Roma e l'altra a Varese) alle ore 8 della domenica mattina seguente. A ripensarci ora, par di sognare!

l'autografia, come mezzo di prova, altri sistemi che assicurassero la provenienza, l'integrità e la riservatezza dei messaggi scritti. Solo così, invero, il pubblico, anche nella versione informatica, li userà con quella sicurezza e fiducia che si esprimevano nel proverbio «carta canta, villan dorme». Si tratta, quindi, di incidere profondamente nelle consuetudini, nelle convinzioni, nella cultura più radicate nella collettività.

Sotto questo aspetto, la disciplina del documento informatico e della firma elettronica va ben al di là del valore tecnico-giuridico di una semplice innovazione settoriale: è una rivoluzione, più che una evoluzione.

Questo obiettivo di così grande importanza è stato, però, raggiunto con una *normativa indubbiamente, a dir poco, contorta*[394], che mette a dura prova le capacità e la collaboratività dell'interprete nel ricostruire un sistema coerente e funzionale e che dimostra emblematicamente quanto sia difficile, non solo coordinare la normativa europea con quella nazionale, ma, prima di tutto, intendere tutti i vantaggi e i rischi che l'informatica può presentare e innestare questa nuovissima risorsa sul vecchio tronco del diritto civile.

[394] Ciò è chiaramente riconosciuto nell'art. 10 della recente legge 29 luglio 2003 n 229 con cui il Governo è delegato ad adottare, entro diciotto mesi uno o più decreti legislativi per il coordinamento e il riassetto delle disposizioni vigenti in materia – tra l'altro – di firma elettronica e di firma digitale «allo scopo di graduare la rilevanza giuridica e l'efficacia probatoria dei diversi tipi di firma elettronica in relazione al tipo di utilizzo e al grado di sicurezza della firma». Speriamo che in tale occasione ci si limiti a chiarire, come qui si è cercato di fare, quanto disposto già, sia pure meno chiaramente, nelle troppe norme già emanate e non si voglia, invece, sconvolgere il sistema da esse scaturito con ulteriori innovazioni.

Capitolo VIII

CONSIDERAZIONI CONCLUSIVE L'INFORMATICA E L'EVOLUZIONE DEL DIRITTO CIVILE

Sommario: 240. Necessità di adeguare il codice civile alla realtà informatica. – 241. Le lacune di fondo del codice civile riparabili con l'informatica. – 242. La «legge-software»: l'edizione informatica del codice civile. – L'uso delle immagini e dei «thesauri» nella redazione della legge.

240. *Necessità di adeguare il codice civile alla realtà informatica.* – Lo studio dell'impatto tra diritto civile e informatica dimostra quanto la disciplina dei singoli istituti giuridici sia stata sempre profondamente influenzata dal modo di vivere della collettività dalla sua mentalità e sensibilità, dai problemi che esso presenta e dai mezzi tecnici che si hanno a disposizione per risolverli, oltreché, ovviamente, dai valori etici dominanti: un insieme di fattori profondamente collegati e in continuo movimento.

Il sistema entra in crisi quando la loro evoluzione non è più sincronica, quando, cioè, si creano sfasature nella velocità del mutamento di ciascuno di essi. Accade, allora, che l'ordinamento giuridico risultante dal loro insieme non venga più sentito come rispondente alle esigenze e alla possibilità del momento, le leggi vengano considerate non più adeguate, più come un peso che non come un fattore di ordinato progresso, in esse non si rispecchi più la coscienza collettiva sicché la loro violazione diventa sempre più frequente e inquietante.

Qualcosa di molto simile ci sembra stia avvenendo in questo scorcio di tempo, a cavallo tra due secoli, l'uno dei quali ha portato tanti cambiamenti di ogni genere – etici, politici, economici, sociali, tecnologici – da lasciare all'altro un compito difficilissimo: quello di ricomporre l'armonia del sistema, quanto meno riducendo – se non proprio annullando – il vallo tra Paese reale e Paese legale.

Per assolvere questo compito ci sembra di primaria importanza adeguare il diritto alla «realtà informatica», cioè al nuovo modo di vivere, di pensare e di sentire che l'uso del computer ha prodotto in

tutto il mondo in questi ultimi quaranta anni, con un ritmo sempre più veloce.

Questo adeguamento non può che cominciare dal diritto civile e, in particolare, dal codice civile che, nonostante la sua ridotta importanza rispetto al secolo scorso per la marea di leggi e «leggine» emanate al di fuori di esso, occupa pur sempre una posizione centrale e decisiva rispetto a tutto il nostro ordinamento.

241. *Le lacune di fondo del codice civile riparabili con l'informatica.* – Se questo è il punto d'inizio, questo adeguamento deve mirare innanzitutto a colmare le lacune più gravi, anche se paradossalmente meno avvertite, di tutta la nostra impalcatura civilistica tradizionale. Rese più evidenti dal confronto con le risorse offerte dall'informatica, due sole di esse appaiono fino ad ora colmate: quella concernente la pubblicità legale delle notizie fornite dalle Camere di Commercio e dal Registro delle Imprese, e l'altra concernente il valore della sottoscrizione autografa dei documenti, ritenuta un pilastro di tutto il nostro ordinamento quantunque, per le ragioni già prospettate, abbia finora retto, non per la sua consistenza (invero solo apparente), ma solo per la buona fede e l'ingenuità della gran massa dei cittadini, quasi sempre restii a contestare l'autenticità della loro grafia e ad evitare così, per il loro onesto comportamento, la paralisi pressoché totale dei giudizi civili.

Ma altri pilastri, che pur dovrebbero esserci, mancano e la loro mancanza è sempre più avvertita e sempre più dannosa. Intendiamo innanzitutto riferirci alla mancanza di strumenti pratici ed affidabili per accertare prontamente, con efficacia «*erga omnes*»:

- chi sia il proprietario attuale di un determinato immobile;
- chi siano gli eredi di una determinata persona;
- ma, innanzitutto: l'identità personale di ciascuno di noi, al di là del nome e del cognome che porta, problema che la globalizzazione della vita rende sempre più arduo e di cui si è già trattato.

È mai possibile che nell'era di INTERNET non si possa ancora sapere con certezza e rapidità chi sia il proprietario di un determinato immobile e chi siano gli eredi di una determinata persona e come siano raggiungibili? Che si debba lasciare alla sagacia di ogni singolo interessato l'onere di accertare da chi sia stata usucapita la proprietà di un immobile, essendo l'usucapione – nonostante l'istituto della trascrizione dei trasferimenti – l'unica roccia su cui fondare il diritto di proprietà? Che si abbia ancora ragione di temere, in molte situazioni, una sostituzione o uno scambio di persona? E come non riconoscere che, qualora tutti i pagamenti avvenissero mediante trasferimento elettronico di denaro, non solo tanti illeciti diventerebbero difficili a compiersi (prima ancora che sanzionabili), ma anche tutti i rapporti interpersonali che implicano trasferimento di denaro (e sono tanti!) diventerebbero più chiari, se non addirittura trasparenti?

L'informatica e la telematica possono oggi risolvere, questi problemi *di fondo*, la cui mancata soddisfacente soluzione condiziona in senso negativo la soluzione di tanti altri problemi derivati e connessi.

242. *La «legge-software»: l'edizione informatica del codice civile.* – Un problema di fondo *di fondo* ancora più essenziale e generale l'informatica può risolvere in relazione alla conoscenza e all'applicazione delle leggi costituenti il nostro ordinamento, diventate ormai così numerose, complesse e farraginose da *non essere più* – come si suol dire – *a dimensione d'uomo*: per convincersene basterebbe ripensare al «pasticcio» legislativo intorno al documento informatico e alla firma elettronica, che ci ha costretto a dedicare all'argomento due sezioni di uno stesso capitolo.

Orbene, tenendo presente che il computer non ha soltanto una smisurata *capacità di memoria* (non inferiore, certo, alle dimensioni pur mostruose raggiunte dalle leggi scritte), ma ha anche una vera e propria intelligenza artificiale e, quindi, una vera e propria *capacità di ragionamento* (vedi al riguardo tutto il capitolo V del libro citato nella prefazione).

Dovrebbe apparire a tutti chiaro che, grazie al computer, *la legge può essere formulata ed applicata in un modo ben diverso da quello attuale, ben più semplice, funzionale e democratico.*

Oggi la legge viene formulata dal Potere legislativo mediante l'enunciazione di regole e di concetti solitamente generali ed astratti, da interpretare poi, per essere applicate ai casi concreti della vita, in varia maniera, a seconda di quanto si ritenga più logico e/o opportuno, sicché quasi mai può parlarsi di interpretazione puramente letterale. Molto più spesso l'interpretazione si rivela o estensiva o restrittiva o sistematica o analogica o storica o funzionale o evolutiva. L'ammissibilità di tutti questi diversi tipi di interpretazione rende l'applicazione della legge il più delle volte incerta ed opinabile, con gravis-

sima e intollerabile compromissione del principio, cardine della Giustizia, secondo cui la legge deve essere eguale per tutti. Ciò perché l'interpretazione del dato legislativo non è, salvo rari casi, opera dello stesso suo autore, bensì di una pluralità di soggetti diversi (quali i giudici, i funzionari delle pubbliche amministrazioni, gli avvocati, i docenti di diritto e ogni altro «*jus peritus*»).

Se poi si tiene conto che una interpretazione non semplicemente letterale del testo ne comporta molto spesso una *integrazione di carattere creativo se non addirittura una correzione* che può spingersi sino ad un capovolgimento completo del significato a tutta prima apparente, allora apparirà anche chiaro che, per effetto dell'ineluttabilità dell'interpretazione, la *tripartizione dei Poteri fondamentali dello Stato ancora a base della nostra Costituzione diventa puramente illusoria*, in quanto i giudici, potendo e dovendo interpretare la legge, sono i veri arbitri di stabilirne l'effettivo contenuto, sicché, contrariamente a quanto sancito nel comma 2 dell'art. 101 della Costituzione, i giudici, a ben vedere, sono *non* «soggetti» alla legge, ma «*al di sopra*» di essa.

Per uscire da questa flagrante contraddizione occorrerebbe formulare la legge in modo così chiaro, inequivoco, completo da rendere non necessaria nessuna altra interpretazione al di fuori di quella puramente letterale, in conformità del noto brocardo «*in claris non fit interpretatio*» e dell'aspirazione di tutti i grandi legislatori: da Mosé a Giustiniano, a San Francesco, a Federico il grande di Prussia, agli illuministi che concepirono il giusrazionalismo.

L'informatica dimostra che tale obiettivo è raggiungibile: il computer, infatti, applica ovviamente alla lettera le istruzioni che riceve col programma per funzionare e, quando il software è accuratamente compilato, la volontà del programmatore si realizza pienamente senza intromissione di interpreti.

Si potrebbe quindi chiedere al legislatore ciò che la tecnologia informatica più avanzata rende possibile: chiedergli, cioè, di *non* continuare a formulare le leggi in modo tradizionale (cioè mediante enunciati generale ed astratti che altri dovrà poi interpretare ed applicare in concreto), ma di provvedere egli stesso (ovviamente con l'aiuto di tecnici informatici) *a trasfondere la propria volontà in un software* e di porre in grado così il computer di applicarla *direttamente* a situazioni di fatto, preventivamente e insindacabilmente accertate da giudici di merito in carne ed ossa.

Il computer diventerebbe, così, una sorta di «datore di responsi» secondo la vecchia formula romanistica «*da mihi factum, dabo tibi jus*», *bypassando* completamente lo scoglio delle possibili diverse interpretazioni ad opera di altri soggetti. In tal modo finirebbe anche la contrapposizione, così viva anche nel mondo del diritto civile, tra «*Interessenjurisprudenz*» e «*Begriffsjurisprudenz*».

Il responso del computer, provenendo direttamente dal «*legislatore-programmatore*», sarebbe soggetto, salva l'impugnazione dei dati di fatto fornitigli in input, soltanto al sindacato della Corte Costituzionale, ove mai le istruzioni del software apparissero costituzionalmente illegittime.

Quasi certamente non pochi, nel prendere atto di una simile proposta, si stracceranno le vesti per lo scandalo, anche se esistono già (e vengono usati da un numero sempre crescente di operatori del diritto) i così detti «*Sistemi esperti legali*» (SEL), grazie ai quali il computer chiede all'utente di fornirgli determinati dati e, sulla base di essi, compila un atto giuridicamente rilevante o pronuncia un «*dictum*» in cui si rispecchia l'interpretazione e l'applicazione della legge. Si pensi, ad esempio, ai softwares oggi in commercio e prodotti da editori giuridici privati che consentono ad un amministratore di condominio di compilare tutti gli atti del suo ufficio previsti dalla legge (e, innanzitutto, dal codice civile) secondo quanto ivi è stabilito o magari deciso dalla giurisprudenza, ad integrazione della legislazione. Analogamente avviene, tanto per fare altri esempi attinenti al diritto civile, in tema di locazioni o per il calcolo degli interessi e della valutazione monetaria[395].

Il ricorso alla giurisprudenza, per risolvere l'operazione di conversione della legge in software, le anfibologie e i vuoti che nella prima spesso si riscontrano, sta facendo slittare sempre più, anche se quasi inavvertitamente, il nostro sistema di «*civil law*» in un sistema di «*common law*». Ma, a prescindere da come apprezzare tale progressivo seppur lento slittamento, mi sembra indubitabile che, fino a che la nostra Costituzione sarà basata sulla tripartizione dei Poteri fondamentali dello Stato, *occorra risolvere il nodo della interpretazione della legge per evitare che, approfittando dell'interpretazione, il potere legislativo passi di fatto dal Parlamento ai giudici*, dando luogo a confusioni e incertezze che possono rivelarsi sotto ogni aspetto esiziali: al punto tale da infondere il coraggio ne-

[395] Cfr. M.G. Losano, *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Einaudi, Torino 1969.

cessario per passare dalla formulazione tradizionale della legge alla «legge software», prodotta dallo stesso legislatore e che applicandosi automaticamente ai fatti specifici prospettati dall'utente del computer, *bypassi* completamente l'insidioso momento della interpretazione[396].

Ovviamente, per riuscire a tanto, occorrerebbe puntare, almeno in un primo momento, su un settore limitato dell'ordinamento, essendo di immane difficoltà fin da subito risolvere il problema del coordinamento di tutte le norme costituenti il nostro ordinamento giuridico: un settore di esso già ben arato dalla dottrina e dalla giurisprudenza, da applicare a fattispecie molto frequenti nella vita di tutti e bene conosciute, quindi, anche dalle persone più semplici anche se prive di cultura giuridica. E quale settore normativo risponderebbe a tali condizioni più del diritto civile, inteso come l'insieme delle disposizioni contenute nel vigente codice civile?

La *conversione del codice civile in un software* dovrebbe, quindi, costituire il primo passo da compiere per un ammodernamento radicale e in senso veramente democratico del diritto.

Non dovrebbero forse le leggi essere formulate nel modo più idoneo, sicuro, semplice ed economico per disciplinare i vari casi della vita? Perché attribuire prima ad un gruppo di persone il compito di formulare delle norme generali ed astratte che, essendo costituite da parole hanno di esse tutta la vaghezza e l'ambiguità, e attribuire poi ad un altro gruppo di persone il compito di trovare le *Tatbestanden* corrispondenti dando alle parole usate un contenuto concreto?

Sappiamo bene che gli illuministi del '700 teorizzarono come garanzia irrinunciabile di giustizia questa separazione di compiti per paura che, nel momento di giudicare un determinato soggetto, lo si assolvesse o lo si condannasse non in base agli stessi criteri valevoli per tutti gli altri componenti della collettività ma, a prescindere da qualsiasi criterio generale, in base al proposito dispotico di favorire o di perseguitare persone determinate, mutando così, solo nei loro confronti, la legge, stabilita per tutti, in una sorta di «*jus singulare*», reso più odioso dal fatto di essere segreto o mascherato dalle motivazioni più ipocrite[397].

[396] Vedi al riguardo la conferenza tenuta da R. Borruso al Consiglio Superiore della Magistratura il 12 dicembre 2001 e pubblicata nel fascicolo n. 2 del 2002 sulla rivista *Il diritto dell'informazione e dell'informatica*, edita da Giuffrè.

[397] Da ricordare in proposito che la parola «privilegio» deriva storicamente dal-

Se, come sembra storicamente dimostrato, lo scopo della tripartizione dei Poteri fondamentali dello Stato, è quello di evitare il dispotismo e il favoritismo, resi possibili dalla libertà di giudicare «caso per caso» senza affatto preoccuparsi che la legge sia applicata, e quindi interpretata, in modo eguale per tutti, allora deve riconoscersi non solo che il rimedio della divisione dei poteri escogitato dagli illuministi non ha conseguito l'obiettivo da essi perseguito (in quanto attraverso il «cavallo di Troia» della libera interpretazione della legge da parte di soggetti molteplici quale è la pluralità dei giudici, il dispotismo e il favoritismo o comunque il soggettivismo e le incertezze normative non sono stati affatto eliminati dalla cittadella del diritto, come si evince da un detto popolare secondo cui «il diritto nei confronti dei nemici si applica e nei confronti degli amici si interpreta»), ma anche che, nell'era del computer, l'imparzialità, l'oggettività e la certezza nell'applicazione del diritto possono essere conseguite in modo del tutto nuovo, più semplice e più garantista: e cioè affidando proprio al computer (e soltanto ad esso) il compito di applicare la legge trasfusa dal legislatore stesso (o, comunque, sotto la sua supervisione) in un software non modificabile in alcun modo da altri soggetti e, quindi, con «output» diverso, da caso a caso, solo per effetto della diversità dei dati di fatto afferenti a ciascun caso e preventivamente comunicati al computer, ma non mai per una diversa interpretazione della legge.

Per raggiungere un traguardo così nuovo ed elevato nella storia del diritto occorrerebbe, però, un ben diverso ed elevato impegno da parte del legislatore: perché un software non si può efficacemente compilare se alla base di esso non vi sono «*idee chiare e distinte*» e se non si approfondisce ciò che effettivamente si vuole mediante la previsione di tutte le ipotesi che normalmente si possono verificare e una regolamentazione espressa per ciascuna di esse: quindi con una disciplina estesa ad una larghissima casisitica. Si tratterebbe, in sostanza, non di fare uno sforzo nuovo, ma soltanto di *anticipare al momento legislativo* quello sforzo di analisi e di approfondimento che oggi viene rimandato in sede di applicazione della norma già emanata con immensa

l'espressione «lex in privos lata», cioè legge emanata per colpire o per favorire una o poche persone e che tali leggi, in sostanza esistono ancora oggi e vanno sotto il nome di «leggi-fotografia» – quando in esse si richiedono tante di quelle condizioni di applicabilità da riferirsi chiaramente solo a predeterminate persone singolarmente considerate.

causazione di contenzioso. Le norme dovrebbero avere il carattere di un vero e proprio «algoritmo» (presupposto essenziale per la compilazione di qualsiasi software), cioè di regole formulate in linguaggio «matematico», nel senso che il loro enunciato sia privo di qualsiasi ragionevole sottinteso, di qualsiasi equivocità, di qualsiasi incompletezza e, perciò, sia costituito da proposizioni elementari connesse secondo i dettami della *logica proposizionale booleana* e formate da parole di significato preciso tratte da uno speciale dizionario solitamente denominato «thesaurus» e creato «*ad hoc*», in modo che il testo sia così chiaro da poter essere applicato da chiunque, *anche dal più sprovveduto*, senza la minima incertezza e il minimo sforzo mentale, previa la c.d. *normalizzazione di linguaggio*. Ed è proprio in questo automatismo l'elevatezza del traguardo che qui si addita perché ancora oggi il diritto è, in pratica, antidemocratico, più a tutela dei forti che dei deboli, dei ricchi che non dei poveri, dei colti che non degli incolti, tanto esso è non raramente astruso e comunque sempre complicato dalla necessità di coordinare tra loro tante norme, pur applicabili ad una medesima fattispecie, ma emanate a distanza di tempo l'una dall'altra e/o disseminate in settori dell'ordinamento molto lontani l'uno dall'altro per diversità della materia generale in ciascuno di essi trattata, sicché, ancora oggi, ben può dirsi – ma lo si deve dire con tristezza – «*vigilantibus succurrunt jura*».

Il diritto non può non essere una scienza degna di studio a livello universitario. Ma l'obiettivo principale di tale scienza dovrebbe essere, non già quello di formare una casta di «mandarini cinesi» monopolizzatori del sapere giuridico, ma piuttosto essere quello di come formulare le norme in modo semplice e breve, usando le parole e i costrutti al tempo stesso più familiari e concisi, tanto da poter essere comprese e rispettate anche dai più sprovveduti, di come facilitare a chiunque la ricerca della norma direttamente applicabile al caso di specie senza necessità di consulenti e, qualora ne risultino più d'una, di come vadano coordinate. Non usare mai una parola di troppo, non cadere mai in ambiguità sintattiche o grammaticali, contenere il numero delle norme entro il limite di quelle che un uomo di media capacità può tenere presenti.

Il punto di arrivo di questa democraticissima direttrice di marcia è, certamente, la «*legge-software*» e il ritorno all'idea illuministica del «codice» come riunione di leggi quantitativamente limitate che si può umanamente pretendere siano rispettate dai più e, perché ciò avvenga, delle quali anche i meno colti e attenti conoscano non dico il

contenuto, ma almeno l'esistenza. Questo «ritorno» è oggi possibile grazie al computer e alla sua prerogativa (esclusiva, nuovissima e ancora da molti, compresi i giuristi, non adeguatamente valutata in tutta la sua enorme potenzialità) di tramutare, per effetto di un appropriato «software», un discorso, contenente precetti e sanzioni qual è quello in cui si estrinseca ogni legge, nella decisione di un caso particolare, superando lo scoglio di interpretazioni non autentiche, cioè provenienti da soggetti diversi dal «*conditor*» della legge stessa.

Una edizione informatica del codice civile (nel senso sopra prospettato) *è la grande occasione da non perdere* per porre su basi, non solo dunque nuove, ma al tempo stesso, più scientifiche e democratiche la materia in esso trattata. La giurisprudenza formatasi sull'interpretazione e applicazione del codice civile è così estesa che non sarebbe difficile al legislatore tenere presenti le fattispecie alle quali dare una concreta risposta e, così, creare un software che tramuti la ricerca e lo studio della legge in un dialogo diretto ed immediato tra il legislatore stesso e ogni interessato alla sicura conoscenza di essa sul piano pratico, in modo da potere agire in un clima di «certezza del diritto», bene essenziale per ogni società che aspiri alla giustizia, all'ordine e al benessere.

Questa prospettiva non è affatto utopistica se si considera che già oggi (e non da oggi bensì ormai da molti anni) il computer è usato da moltissimi operatori del diritto (magistrati, avvocati, notai, commercialisti, funzionari della PA, consulenti) per ricercare nelle banche-dati automatizzate di documentazione giuridica le leggi, la giurisprudenza, la dottrina pertinenti a fattispecie legali particolari e che tale ricerca è proficua solo se e nella misura in cui la domanda posta al computer dal ricercatore sia «capita» dal computer nei suoi giusti termini grazie a softwares sempre più sofisticati e tesi al raggiungimento di una vera e propria «intelligenza artificiale»[398] per effetto della quale il linguaggio umano sia sempre più completamente compreso dal computer[399]. Il passo ancora da compiere sarebbe quindi relativamente modesto: si tratterebbe di realizzare un software che dai documenti «pertinenti» selezionati sulla questione indicata dal ricercatore sapesse estrarre le decisione da adottare.

[398] Vedi di G. Sartor, *Intelligenza artificiale e diritto*, Giuffrè, Milano 1996.

[399] Vedi al riguardo l'interessantissima evoluzione che, presso il Centro Elettronico di Documentazione Giuridica della Corte di Cassazione, sta subendo in questi ultimi mesi il sistema di ricerca ITALGIURE.

Tanto per fare un esempio di come potrebbe funzionare un sistema basato su «legge-software», si pensi a chi voglia fare testamento. Comunicata tale sua intenzione al computer, quest'ultimo gli chiederebbe subito se sia maggiorenne e se abbia una volontà libera e consapevole. Ottenuta risposta affermativa, gli chiederebbe se voglia rivolgersi a un notaio oppure no: se, in altri termini, voglia fare un testamento pubblico ovvero segreto ovvero olografo, spiegandogli la differenza tra queste diverse forme.

Posto che il testatore abbia prescelto la forma dell'olografo, il computer gli chiederebbe se intenda dispensare ciascuno dei suoi successori dall'obbligo di imputarsi, ai fini del calcolo della quota di riserva, le donazioni e i legati o, ai fini della collazione, le donazioni (dirette o indirette), di indicare tutti i suoi beni mobili o immobili e il valore pecuniario attribuito a ciascuno di essi, a chi voglia attribuirli (indistintamente o quali e in che misura), la composizione della sua famiglia (coniuge, discendenti, ascendenti), quali donazioni abbia fatto in precedenza, se intenda attribuire a ciascuno dei suoi successori la qualifica di erede (cioè di successore a titolo universale) o di legatari (cioè di successore a titolo particolare) (con illustrazione dei diversi effetti in relazione al pagamento dei debiti), se voglia apporre delle condizioni, e di che tenore, alle sue disposizioni, se, infine, queste ultime comprendano la totalità dei beni posseduti dal testatore o se ve ne siano altri in relazione ai quali lascia che la loro attribuzione avvenga secondo le norme delle successioni legittime e quindi a beneficio del parente più prossimo entro il sesto grado.

Ricevute tutte queste informazioni (o «dati» che dir si voglia), il computer stesso potrebbe stendere un progetto di testamento ad esse conforme, raccomandando, a chi lo voglia fare suo, di trascriverlo, previa verifica di effettiva rispondenza alla propria volontà, tutto di proprio pugno su un foglio di carta apponendo, su di esso, data e sottoscrizione. Qualora i «dati» forniti al computer non permettessero di rispettare legalmente le intenzioni (come, nel caso in cui risultassero violate le norme di legge sulle quote di riserva in favore dei legittimari), il computer, si limiterebbe ad indicarne le ragioni.

Questo è soltanto un esempio molto abborracciato di come potrebbe funzionare una «*legge software*» perché la sua realizzazione dovrebbe, ovviamente, essere frutto del più attento e approfondito studio da parte di una folta schiera di pratici e di teorici del diritto nonché di tecnici della programmazione informatica come «*equipe*» di supporto al legislatore. Un grande impegno certo: ma quanto si

faciliterebbe l'inesperto del diritto a mantenersi nei binari della legalità, quanto si ridurrebbero le controversie, quanta più credibilità acquisterebbero le istituzioni, posto che, almeno per quanto concerne l'applicazione e l'interpretazione delle norme, l'imparzialità (che è poi il fine ultimo della tripartizione dei Poteri dello Stato) sarebbe assicurata! Ai giudici non rimarrebbe che accertare i fatti presupposti dalla norma: cioè la «protasi» del giudizio, posto che l'«apodosi» (cioè la conclusione) sarebbe tratta direttamente dal computer. In tal modo i processi sarebbero molto più trasparenti e molto più rapidi e, pur tuttavia, il loro svolgimento, diviso in due fasi nettamente distinte (rivolte l'una alla fissazione della «*regola juris*» e l'altra all'accertamento dei fatti rispetto ad essa rilevanti), a ben vedere, non sarebbe altro che un paradossale ritorno al passato: al passato glorioso del diritto pretorio romano che si estrinsecò nel *processo formulare* in cui si distingueva una prima fase (detta «*in jure*» diretta alla precisazione della questione da risolvere («*litis contestatio*») e che si concludeva con la designazione di un giudice («*judex*») privato per l'accertamento dei fatti in essa dedotti o con l'esposizione del principio di diritto («*formula*») sotto forma di una specie di programma cui egli avrebbe dovuto attenersi per decidere la causa, e una seconda fase («*ope judicis*») in cui i fatti predetti dovevano essere accertati con la conseguente condanna o assoluzione del convenuto.

243. *L'uso delle immagini e dei «thesauri» nella redazione della legge.* – L'«intelligenza artificiale»[400], da dare al computer per porlo in grado di applicare automaticamente la legge, potrebbe essere realizzata non solo mediante la «*formalizzazione*» del linguaggio normativo (sì da trasformare il testo delle leggi in veri e propri algoritmi), ma anche mediante l'uso di *immagini*, (costituite da disegni, fotografie, filmati) assunte come modello cui conformare determinate situazioni o cose o comportamenti o, quanto meno, la loro qualificazione giuridica mediante una serie di confronti da eseguirsi per riscontro di identità, sia pure tollerando margini di diversità giudicati non significativi in relazione alle fattispecie che interessano.

L'introduzione dell'immagine nella formulazione della legge e, quindi, nella sua applicazione automatica comporterebbe un vero e

[400] Vedi il libro di G. Sartor, *Intelligenza artificiale e diritto*, Giuffrè, Milano 1996.

proprio «salto di qualità» della funzione che alla legge deve essere riconosciuta, a tutto vantaggio della comprensibilità per tutti delle sue prescrizioni e della oggettività della sua applicazione e, quindi, della certezza del diritto, bene irrinunciabile di ogni società civile, giusta e progredita. È, infatti, appena il caso di tornare a ripetere che le leggi devono essere formulate non per costituire una palestra di esercitazioni ermeneutiche che diano ai giudici modo di mostrare tutto il loro acume e, comunque, di esercitare un potere preminente sopra ogni altro, ma per garantire il *pari trattamento* di tutti i cittadini che si trovino in determinate condizioni *quale che sia il giudice che abbiano la ventura di avere*.

Le parole non sono sufficienti a fornire tale garanzia perché le frasi del discorso alle quali il loro insieme dà luogo possono risultare ambigue per effetto di tre fattori nessuno dei quali è ancorato, nel linguaggio naturale, al rispetto di regole precise: la sintassi, la grammatica e la semantica.

È ben vero che alle ambiguità della sintassi e della grammatica almeno in parte può rimediarsi mediante la struttura della logica formale (*algebra preposizionale di Boole*), operatori quantificazionali, logica deontica: vedi in proposito §§ 48/51 del libro citato nella prefazione di cui si è già parlato diffusamente a proposito della interpretazione del contratto.

Restano, però, le ambiguità della semantica (cioè del significato da attribuirsi alle singole parole)[401] che non sono spesso superabili neppure attenendosi alle definizioni che, per ciascuna di esse, si trovano sui più accreditati dizionari, peraltro non sempre concordi e comunque sforniti di «*auctoritas cogente*», ripetendosi spesso l'incertezza del vocabolo da definire nei vocaboli usati per definirlo. D'altra parte, all'infuori del significato emergente da tali dizionari, quale potrebbe essere il «significato proprio della parola» da attribuire ad essa in conformità della sibillina disposizione di cui all'art. 12 delle preleggi? Si può certo obiettare che, se la parola, da un lato, può ricevere interpretazioni diverse, dall'altro lato essa si presta, per il suo carattere molto spesso generale ed astratto, ad essere «*inverata*» in una pluralità indefinibile «a priori» di tante situazioni od oggetti diversi pur nella comunanza di qualche elemento, sicché si presta, proprio per questo suo presunto difetto, ad esprimere i concetti legislativi nel modo più economico possibile, cioè, molte volte, con una sola parola. Ma si può controbiettare che, con le più aggiornate tecniche eidomatiche, si può far apparire sullo schermo di un computer una serie grandissima di *immagini diverse* ricavate automaticamente da una immagine-base come se si trattasse di «variazioni su tema» e, quindi, ricomprensive di tutte quelle situazioni o quegli oggetti che una sola parola è in grado di evocare, sicché si avrebbero nel contempo precisione, oggettività di riferimenti e molteplicità di fattispecie previste.

[401] Cfr. il § 25 del libro di R. Pagano, *Introduzione alla logistica*, Giuffrè, Milano 2001.

Comunque, anche a prescindere dal ricorso alle immagini per rendere più cogente e chiaro il linguaggio legislativo, resterebbe pur sempre la possibilità di usare il computer per fare il censimento delle parole usate dal legislatore, cominciando ovviamente da quelle usate nel codice civile, per attribuire poi a ciascuna di esse mediante opportune definizioni da darsi sempre in sede legislativa, un significato preciso o, quanto meno, meno vago di quello che astrattamente possono avere. Si dirà che mediante la formazione di siffatti dizionari (ai quali in informatica si dà solitamente il nome di «thesauri») verrebbe cristallizzato il linguaggio e, con esso, l'opera creativa, adattativa ed evolutiva svolta oggi dall'interprete, libero, come è, di estendere o restringere o modificare il comune significato delle parole. *Ma la certezza del diritto è un bene avente un valore ben maggiore di quello riconoscibile ai suoi interpreti.* Infatti, come l'Uomo non è al servizio per il Sabato, ma il Sabato è al servizio dell'Uomo, così, analogamente, le esigenze di tutta la collettività che si rispecchiano nel diritto devono prevalere sulla conservazione delle posizioni dominanti fino ad ora riconosciute a «scribi e glossatori». Altrimenti, sarebbe come se, pur di conservare l'alta funzione sociale e scientifica dei medici, si osteggiasse la prospettiva di una popolazione ormai immune da qualsiasi malattia.

Il lungo cammino della storia del diritto, *a cominciare dal diritto civile*, non può non avere oggi altro traguardo più luminoso di quello che l'uso del computer rende intravedibile mediante l'applicazione automatica della legge a situazioni di fatto preventivamente accertate: un diritto assolutamente certo e sicuramente imparziale, fruibile, in tempo reale e senza alcun costo, anche dalla persona più sprovveduta: un diritto veramente democratico.