

UNIVERSITA' DEGLI STUDI DI PARMA

FACOLTÀ DI GIURISPRUDENZA

LA FIRMA DIGITALE

di

MASSIMO FANTIN

Dipartimento: DIRITTO COMMERCIALE

Relatore: GUIDO UBERTO TEDESCHI

Laureando: MASSIMO FANTIN

Anno Accademico: 1999 - 2000

“Inequissimum videtur cuique scientiam
alterius quam suam nocere, vel
ignorantiam alterius alii profuturam”

Ai miei genitori e a Giovanni

Parma, 13 ottobre 2000

SOMMARIO

Introduzione.....[I]

CAPITOLO I: *Dalla sottoscrizione autografa alla c.d. firma digitale.*

1. Le garanzie fornite dalla sottoscrizione autografa nel nostro ordinamento.....[1]
2. Trattamento giuridico del documento informatico prima della c.d. “Bassanini-uno”.....[8]
3. Crittografia simmetrica e asimmetrica.....[20]
4. Firma digitale e sottoscrizione: analogie e differenze sostanziali.....[34]

CAPITOLO II: *La firma digitale in Italia.*

1. Quadro di riferimento normativo.....[42]

2. Il documento informatico: requisiti, validità e efficacia probatoria.....
..[58]
3. - (*segue*) scrittura privata informatica e prova legale.....[68]
4. - (*segue*) il c.d. principio del “non – ripudio”.....[83]
5. L’art. 60 del D.P.C.M. 08/02/99.....[96]
6. Copie di atti e documenti in forma elettronica.....[108]
7. Libri e scritture contabili.....[120]
8. Il *key escrow* facoltativo.....[127]
9. Firma digitale autenticata.....[136]
10. Atto pubblico notarile digitale.....[145]

CAPITOLO III: *Ordinamento comunitario e firma digitale*

1. Analisi della direttiva 1999/93/CE del Parlamento e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.....[155]

CAPITOLO IV: *Considerazioni e valutazioni conclusive*...[169]

Appendice legislativa.....

- **L. 15 marzo 1997, n.59.**- Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (Articolo estratto).....
- **D.P.R. 10 novembre 1997, n. 513.**- Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.....
- **Relazione di accompagnamento al D.P.R. 513/97**.....
- **D.P.C.M. 8 febbraio 1999.** - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del

Decreto del presidente della Repubblica, 10 novembre 1997,
n.513.....

- **Direttiva 1999/93/CE del Parlamento e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.....**

Bibliografia.....

INTRODUZIONE

Con l'art 15 della L. 59/97 può dirsi conclusa la più che decennale *querelle* che aveva coinvolto la dottrina circa la natura giuridica del documento informatico rispetto a quello cartaceo, e soprattutto circa l'autografia che, fino a non molto tempo fa, era considerata da gran parte della dottrina quale requisito implicito della sottoscrizione richiesta dal legislatore del '42 come mezzo necessario per imputare la volontà incorporata nel documento al suo autore.

La L. 59/97, all'art.15, e i successivi D.P.R. 513/97 et D.P.C.M. 08/02/99 relativi alla cd. firma digitale, stabilendo che il documento informatico è “valido e rilevante a tutti gli effetti di legge”, hanno introdotto nel nostro ordinamento una vera e propria rivoluzione copernicana capace di modificare radicalmente il modo con cui vengono gestiti i rapporti fra privati e fra questi e la P.A.

In particolare, un documento informatico dotato di firma digitale offre le stesse garanzie che offrirebbe un “tradizionale”

documento cartaceo con sottoscrizione autografa relativamente all'individuazione di eventuali alterazioni successive al testo originario (c.d. *integrità* del documento) e in relazione alla *imputabilità* all'autore del documento della volontà incorporata nel medesimo.

Grazie a questo sistema di firma è oggi possibile attribuire al documento informatico il valore di scrittura privata (art. 2702 cc.) e, a certe condizioni, quello di scrittura privata autenticata (art. 16 D.P.R. cit. e art. 2703 c.c.).

Ma il legislatore si è spinto più in là riconoscendo una limitata efficacia probatoria anche al documento informatico che, seppur sprovvisto di firma digitale, sia "munito dei requisiti" previsti dal D.P.R. 513/97 e dal D.P.C.M. 08/02/99.

Così disponendo l'art 5, comma 2, del D.P.R. 513/97, resta invero da chiedersi quale trattamento probatorio sia riservato ai documenti informatici non in regola con i requisiti previsti dal regolamento stesso o sottoscritti con sistemi di firma digitale diversi da quelli previsti dal nostro legislatore (mi riferisco al P.G.P.).

Ma la vera novità è il riconoscimento della validità di un “sistema di imputabilità indiretto” che diversamente dal sistema tradizionale, basato su un rapporto fisico tra sottoscrittore e documento incorporante la sua volontà (rapporto verificabile tramite le scienze calligrafiche, presumendosi la sottoscrizione autografa unica per ogni individuo), si basa sul meccanismo del non-ripudio: in altre parole, sull'impossibilità per un soggetto di negarsi autore di un documento informatico cui sia stata apposta la sua firma digitale.

Parlo di imputabilità indiretta perché il documento elettronico deve essere inteso, in linea generale, come il documento prodotto dall'elaboratore elettronico. Il fatto che ci sia un “filtro” tra soggetto dichiarante e dichiarazione, non esclude che il primo sia l'autore della seconda e ciò in base al meccanismo sopra delineato.

La firma digitale come “risultato della procedura informatica basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica,

rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico..." (art. 1, lett. b) del D.P.R. 513/97) svolge in definitiva la stessa funzione della sottoscrizione tradizionale (imputabilità più integrità del documento affidata alla materialità stessa del supporto) pur essendo tanto immateriale quanto il documento elettronico.

La funzione della firma digitale, sotto il profilo della garanzia dell'integrità del documento, non è quella di creare documenti indelebili (essendo il documento informatico manipolabile per definizione!) ma quella di rendere riconoscibile ogni modifica, anche di un solo bit, all'originale firmato senza la necessità di ricorrere a complicate perizie calligrafiche.

Anzi, la sicurezza raggiungibile diventa forse maggiore rispetto alla verifica tradizionale di una sottoscrizione autografa.

Un ultimo dato: nel nostro codice civile esiste una norma, l'art.2705, che attribuisce la stessa efficacia della scrittura privata al telegramma consegnato o fatto consegnare dal mittente pur in difetto di sua sottoscrizione. Una lettura attenta di tale articolo denuncia la consapevolezza del legislatore di allora circa

l'inadeguatezza del sistema della sottoscrizione, intesa quale mezzo di imputabilità diretta, a favore di altre soluzioni che, in situazioni particolari, garantissero comunque la possibilità di accertare in modo univoco la paternità di un documento.

È la funzione di imputabilità soggettiva di un atto al suo autore che doveva (e deve!) essere assicurata, con il mezzo di volta in volta più idoneo rispetto alle forme e alla celerità con cui la “volontà negoziale” di un soggetto doveva raggiungere (*rectius*: si voleva raggiungesse) la controparte.

E a queste, oramai diffuse, esigenze di celerità nella trasmissione della “volontà negoziale”, il legislatore ha risposto, assicurando la funzione ma innovando nel mezzo che ora consiste principalmente nella “esclusività dell'apparato tecnico”.

CAPITOLO I

DALLA SOTTOSCRIZIONE AUTOGRAFA ALLA C.D. FIRMA DIGITALE

1. LE GARANZIE FORNITE DALLA SOTTOSCRIZIONE AUTOGRAFA NEL NOSTRO ORDINAMENTO

Nell'ambito dei rapporti privatistici (*rectius*: delle scritture private) la sottoscrizione, da intendersi come “apposizione su di un documento¹ della propria firma autografa²”, attua quel meccanismo di *imputabilità diretta* voluto dal legislatore per assicurare la paternità della dichiarazione negoziale incorporata nel documento al suo autore.

¹ Per documento deve intendersi “la cosa rappresentativa cioè capace di rappresentare un fatto”: così CARNELUTTI, *La prova civile*, 2° ed., Roma 1947, pagg. 183 ss. Non è necessario che il fatto rappresentato sia anche giuridicamente rilevante, come sostiene ad esempio ANGELICI, (*Documentazione e documento*, in Enc. Giur. Treccani, XI, Roma 1989, I) dato che un fatto non giuridicamente rilevante *ab-initio* potrebbe diventarlo successivamente e acquisire quindi efficacia probatoria.. Requisito ontologico del documento, idoneo a garantirne la funzione rappresentativa, si riteneva essere la sua *materialità* (vedi CANDIAN, voce *Documentazione e documento* –teoria generale-, in Enc. dir., Milano, 1964, vol. XIII, pag.579 ss. che definisce il documento come “ oggetto corporale, prodotto dall'uomo al fine di conservare le tracce dell'attività dell'uomo stesso e degli eventi che lo interessano”), difettando la quale sarebbe stato impossibile, secondo dottrina anche recente, garantire l'integrità del documento alla luce di alterazioni successive al testo originario ponendo quindi gravi problemi in ordine alla paternità della scrittura (così ORLANDI, *La paternità delle scritture*, Milano 1997, pagg.100-103 in relazione alla intrinseca manipolabilità del supporto informatico, ma prima dell'adozione da parte del nostro legislatore di un sistema crittografico a chiavi asimmetriche.).

² Circa l'essenzialità o meno dell'autografia della sottoscrizione vedi *infra* in questo stesso paragrafo.

Requisiti della sottoscrizione secondo la dottrina tradizionale⁽³⁾ sono:

- La *nominatività*, dovendo la sottoscrizione esplicitare il nome e il prenome (art. 6² c.c.);
- La *leggibilità*, in quanto consti di una struttura grafica comprensibile da parte di chiunque legga;
- La *riconoscibilità*, in quanto idonea ad identificare gli autori dell'atto contenuto nel documento⁽⁴⁾;
- La *non-riproducibilità*, essendo la firma legata indissolubilmente al documento, di regola cartaceo, incorporante la volontà negoziale.

A mente l'art. 2702 c.c. vediamo che la scrittura privata, da intendersi come “qualunque documento scritto e sottoscritto dalle parti con firma autografa”, fa piena prova della *provenienza* delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta, salvo che la scrittura sia impugnata con querela di falso.

⁽³⁾ Così CARNELUTTI in *Studi sulla sottoscrizione*, in Riv. dir. comm., I, 1929 richiamato da DEL VECCHIO in *Riflessioni sul valore giuridico della sottoscrizione elettronica*, Riv. Not., 1991. Relativamente all'ultimo requisito cfr. ZAGAMI in *Firme digitali, crittografia e validità del documento elettronico* in Riv. dir. inf., 1996.

⁽⁴⁾ A parere di chi scrive quest'ultimo requisito è superfluo essendo in realtà la risultante della combinazione dei primi due. Infatti, una sottoscrizione che sia nominativa e leggibile implica necessariamente la riferibilità della volontà negoziale incorporata nel documento al suo sottoscrittore.

La sottoscrizione è legalmente considerata come riconosciuta se autenticata da notaio o da altro pubblico ufficiale a ciò autorizzato (art. 2703¹ c.c.).

Gli artt. 2703-2704 c.c. devono poi essere coordinati con gli artt. 214 ss. del c.p.c. secondo i quali la sottoscrizione comporta che la parte contro cui la scrittura è prodotta in giudizio abbia un *onere di disconoscimento*, inadempito il quale si verifica il riconoscimento tacito (art. 215 c.p.c.) e la scrittura è legalmente considerata come riconosciuta.

Se il disconoscimento avviene entro i termini e con le modalità fissate dall'art. 215 c.p.c. alla parte che ha prodotto in giudizio la scrittura viene offerta l'alternativa tra il rinunciare ad avvalersi dello scritto disconosciuto; oppure insistere nel sostenere la provenienza dalla controparte, affrontando così un giudizio *ad hoc*^{5D}.

Da un'analisi appena attenta delle norme sopra riportate emerge con chiarezza l'importanza che la sottoscrizione assume nell'impianto codicistico del '42: essa, infatti, può venire in considerazione sia come elemento essenziale del negozio (si parla in tal caso di sottoscrizione-forma, argomentando ex art. 1325 n°4) sia come elemento essenziale del documento.

Sotto quest'ultimo profilo essa conferisce la paternità del documento ed assicura l'adesione al testo, donde l'imputabilità del dichiarato al

^{5D} L'istanza di verificaione ex art. 216 c.p.c. può proporsi tanto in via incidentale che con autonomo atto di citazione. Si tratta in ogni caso di un giudizio di accertamento avente ad oggetto l'autenticità della scrittura o della sottoscrizione disconosciuta.

sottoscrittore in quanto si presume che colui il quale sottoscrive il documento lo abbia letto e lo abbia trovato conforme alla sua volontà⁶.

Anche la Cassazione in una sua recente pronuncia⁷ sembra confermare questa linea di pensiero. Infatti, secondo la Suprema Corte: " ...le scritture prive della sottoscrizione non possono rientrare nel novero delle scritture private aventi valore giuridico formale con effetti sostanziali e probatori neppure quando non ne sia stata impugnata la provenienza dalla parte a cui vengono apposte; la parte contro la quale queste scritture sono prodotte non ha, conseguentemente l'onere di disconoscerne l'autenticità ai sensi dell'art. 215 c.p.c., che si riferisce solo al riconoscimento della sottoscrizione, questa essendo, ai sensi dell'art. 2702 c.c., il solo elemento grafico in virtù del quale, salvi i casi diversamente regolati (artt. 2705, 2707, 2708, 2709 c.c.) la scrittura diviene riferibile al soggetto da cui proviene e può produrre effetti a suo carico."

A inizio paragrafo ho fornito la definizione tradizionale di sottoscrizione come "l'apposizione su di un documento della propria firma *autografa*".

L'*autografia* è sempre stata considerata dalla dottrina tradizionale come componente direi "ontologica" della sottoscrizione; questa convinzione era

⁶ Così DEL VECCHIO in *Riflessioni sul valore giuridico della...* cit.

⁷ CASS- Cass., sez. II, 02-10-1996, 8620/1996 Soc. Trussardi – Ditta Badi Abul Huda Radwan, in *Mass.*, 1996

talmente radicata da portare ad affermare: "Firma ha da essere, quindi *deve* essere manoscritta"⁽⁸⁾.

E l'equazione "firma = autografia" in tanto si riteneva essere principio generale in quanto diretta è la riconducibilità all'identità di colui che la appone, essendo la calligrafia un elemento identificativo della persona, dotata dei caratteri della unicità e conseguentemente della sua verificabilità⁹.

A sostegno di tale tesi¹⁰ venivano richiamate puntuali norme, che avrebbero dovuto evidenziare come la sottoscrizione autografa risulti privilegiata dal legislatore: l'art. 602 c.c. (in tema di formalità del testamento pubblico e del testamento segreto), gli artt. 1 n.8 e 100 n.7 della legge cambiaria, l'art. 1 n.6 della legge sull'assegno bancario, l'art. 2702 c.c. relativo alla disciplina della scrittura privata e così via.

Ma così argomentando si poneva come fondamento della dimostrazione ciò che si voleva dimostrare, formulando quindi una petizione di principio.

⁽⁸⁾ Così VIVANTE, *Trattato di diritto commerciale*, V ed., 1928, vol. III, p.227 richiamato da L. SALAMONE in *Sottoscrizione meccanica e firma dei titoli cambiari*, Banca-Borsa.... 1996, II, p.83 ss.

⁹ Cfr. MORELLO, *Sottoscrizione*, in *Noviss. Dig. It.*, XVII, 1970, p. 1004.

¹⁰ Si ricordano fra i tanti, seppur nell'ambito dei titoli cambiari e senza pretese di esaustività, A.PAVONE-LA ROSA, *La cambiale*, in *Trattato CICU-MESSINEO*, Milano,1994, p. 82 sgg. et L. SALAMONE, *Sottoscrizione meccanica e firma dei titoli cambiari*, in *Banca, borsa ecc.* 1996, II, p. 83 ss. che testualmente cito: "Siccome del massimo di verità è accreditabile la firma autografa, può pensarsi che l'autografia sia un principio generale". Dello stesso orientamento anche la gran parte della giurisprudenza di allora: cfr. Trib. Torino 26 ottobre 1994, in *Banca, borsa ecc.* 1996, II, p.71 ss. Tuttavia *contra* CHIOMENTI già in *Giust. Civile*,1976, I, pp. 54-55 quindi in *Il titolo di credito: fattispecie e disciplina*, 1977, pp. 291-296 e dopo la legge "Bassanini" in *Giust.Civile* 1998, pp. 725-732 dove sostiene la non necessaria equivalenza sottoscrizione=autografia, quale principio generale dell'ordinamento giuridico, perché di tale equivalenza non si trova traccia nel codice civ. e perché quando il legislatore vuole per la validità di determinati atti la sottoscrizione autografa lo richiede espressamente (arg. ex art.602 cod.civ.).

Anzi, le stesse norme su citate potevano essere lette in senso contrario, come consapevolezza da parte dello stesso legislatore dell'eccessiva rigidità del principio legato all'autografia. Così, ad esempio, lo stesso art. 602 c.c. dispone che la sottoscrizione, benché "informale" (cioè non rispettosa del requisito della nominatività sopra riportato) resta valida purché sia idonea a designare con certezza la persona del testatore¹¹.

Non esiste alcuna norma nel nostro codice che prescriva una forma valida *semper et semper* per la sottoscrizione e la ragione sta in ciò: che, vigente nel nostro ordinamento il principio della libertà delle forme (arg. ex art. 1325 n. 4 c.c.), ne discende che là dove la firma non è richiesta con particolare formalità, essa è libera¹²: l'unico vincolo è il rispetto della funzione cui la sottoscrizione è preordinata.

Ne consegue che se importante è la funzione e non il mezzo attraverso cui la funzione (c.d. di *imputabilità*¹³) è garantita, allora può senza dubbio

¹¹ Cfr. DEL VECCHIO *op. cit.* e CHIOMENTI *op. cit.* Alle stesse conclusioni si perviene dopo la lettura del dispositivo dell'art. 8 legge cambiaria che ammette la deroga al principio della nominatività della sottoscrizione in favore della c.d. "siglatura". Vedi anche l'art. 2354 c.c. che dichiara valida la sottoscrizione mediante riproduzione meccanica della firma sui titoli azionari, purché l'originale sia depositato presso l'ufficio del registro delle imprese ove è iscritta la società.

¹² "Libera" anche di non esserci affatto se viene comunque garantita *aliunde* la c.d. funzione di *imputabilità* cui la sottoscrizione è preordinata (arg. ex art. 2705 c.c.). Cfr. quanto brevemente riportato in ordine all'esegesi di quest'articolo nell'introduzione, p.VI-V.

¹³ Ho voluto utilizzare quest'unico termine come assorbente le tre componenti funzionali che CARNELUTTI, in *Studi sulla sottoscrizione*, cit., attribuisce alla firma. In particolare la sottoscrizione ha essenzialmente:

- Una funzione *indicativa*, consistente nell'identificare l'autore del documento;
- Una funzione *dichiarativa*, consistente nell'assunzione di paternità del documento da parte dell'autore dello stesso;
- Una funzione *probatoria*, in quanto mezzo per provare l'autenticità del documento.

ammetersi la legittimità di forme di sottoscrizione diverse, anche *strutturalmente*, da quella tradizionale.

La c.d. firma digitale può quindi considerarsi in rapporto di specie a genere rispetto alla firma tradizionale, perché di quest'ultima soddisfa tutti i requisiti oltre che identità di funzione. Probabilmente il dato più curioso, relativamente all'argomento trattato in questo paragrafo, e che dopo il D.P.R. 513/97 ad una nominatività tradizionalmente intesa si è ufficialmente affiancata una "*nominatività elettronica*".

2. TRATTAMENTO GIURIDICO DEL DOCUMENTO INFORMATICO PRIMA DELLA C.D. "BASSANIN-UNO"

L'art. 15, secondo comma, della L. 59/97 (e i successivi regolamenti di attuazione) riconoscendo validità e rilevanza, a tutti gli effetti di legge, al documento informatico e soprattutto al contratto in forma elettronica, ha introdotto nell'ordinamento privatistico italiano una novità di assoluto rilievo che, se da un lato ha fatto propri i risultati dell'elaborazione dottrinale relativamente alla natura giuridica del documento elettronico, dall'altro ne ha superato i contrasti riguardanti l'impossibilità ad attribuirgli la natura giuridica di scrittura privata ex art. 2702 c.c..

Appare, preliminarmente, opportuno soffermare l'attenzione su alcuni concetti giuridici-base, aventi ad oggetto il documento e l'attività di documentazione, per poi passare in rassegna le più significative posizioni dottrinarie che, prima dell'intervento del legislatore, hanno conferito dignità giuridica al documento elettronico.

Punto di riferimento obbligato per la definizione dei concetti giuridici di documento e documentazione rimane l'opera di Francesco Carnelutti¹ che, sebbene integrata da successivi interventi dottrinari² e giurisprudenziali, conserva ancora piena validità

¹ CARNELUTTI, *Documento (teoria moderna)*, in Noviss. Dig. It., VI, 1975, p. 85 ss.

² Fra i numerosi interventi, e senza pretesa di esaustività, ricordo: CANDIAN, *Documentazione e documento*, in Enc. Dir., XIII, 1964, p.579 ss.; IRTI, *Sul concetto giuridico di documento*, in Studi sul

Tra le varie definizioni di documento elaborate dalla dottrina³³ emergono tre costanti: da un lato la *materialità* del supporto destinato ad incorporare la rappresentazione di un fatto, dall'altro l'utilizzazione di *segni*³⁴ con funzione descrittiva del fatto stesso, cui segue il requisito dell'idoneità del supporto a *durare nel tempo* (durata che può essere anche brevissima, non esistendo norma di legge che prescriva in tal senso).

Inoltre, è dato rilevare che, in nessuna delle definizioni riportate in nota, si sia richiesta la natura cartacea del supporto quale attributo necessario e qualificante il requisito della materialità del documento³⁵.

formalismo negoziale, 1997, p.159 ss.; DEL VECCHIO, *Riflessioni sul valore giuridico della sottoscrizione elettronica*, in Riv. Not., XLV, 1991, p.986 ss.; MONTESANO, *Sul documento informatico come rappresentazione meccanica della prova civile e nella forma negoziale*, in Riv. dir. proc. civ., 1987, p.1 ss.; ANGELICI, *Documentazione e documento* (diritto civile), in Enc. giur. Treccani, 1989; DI SABATO, *Il documento contrattuale*, 1997.

³³ Documento è stato così definito:

- “cosa che rappresentativa di un fatto”: CARNELUTTI, *Documento* (teoria moderna), cit.
- “cosa corporale, semplice o composta, idonea a ricevere, conservare, trasmettere, la rappresentazione descrittiva o emblematica o fonetica di un dato ente giuridicamente rilevante: CANDIAN, *Documentazione e documento*, cit., p.579
- “*res signata*, onde è dato pronunciare il giudizio di esistenza di un fatto, che sia sussumibile sotto un tipo normativo”: IRTI, *Sul concetto giuridico di documento*, cit., p.196
- “qualsiasi supporto visivi, fonico, magnetico o cartaceo sul quale sono impressi segni comunicativi in grado di essere percepiti dall'uomo direttamente o attraverso l'impiego di particolari strumenti”: DI SABATO, *Il documento contrattuale*, cit.

³⁴ I segni, come è dato riscontrare nella definizione di documento data dal DI SABATO, non devono essere necessariamente grafici (nel qual caso ci troveremmo di fronte ad una dichiarazione), ma possono assumere qualsiasi forma, purché idonea a rappresentare un fatto. *I segni peraltro non devono essere dotati del requisito della immediata intelligibilità, potendo quest'ultima essere il risultato di una procedura di decifrazione.*

³⁵ Di quanto detto può trovarsi riscontro anche nella legge. Infatti una lettura, anche superficiale, dell'art. 1 del R.D. 1666/37 disciplinante la facoltà del notaio di “ricevere in deposito atti pubblici (...), scritture private, *carte e documenti*” evidenzia come anche il legislatore fosse ben consapevole della possibile differenziazione tra le varie forme che può assumere la materialità del documento. Così, CAIÒ, *Ammissibilità del deposito di software presso un notaio*, in Cons. Naz. Not., Studi e materiali, I, 1986, p.418 ss.

Altra distinzione ricorrente in dottrina è quella fra documento e documentazione: distinzione che porta a identificare l'attività di documentazione con il concetto di *forma* del negozio giuridico⁷⁶.

Infatti, il supporto (*res*) diventa documento (*res-signata*) solo a seguito dell'attività consistente nell'apposizione di segni: pertanto mentre il documento, come risultato di tale attività, attiene al profilo probatorio, l'attività di "scritturazione" (da intendersi in senso ampio) attiene al profilo della forma del negozio giuridico.

Con particolare riferimento alla forma scritta⁷⁷ (art. 1350 c.c.), si distingue fra atto pubblico e scrittura privata; quest'ultima è disciplinata agli artt. 2702 ss. c.c. dal punto di vista della sua efficacia, ma di essa il codice non contiene alcuna definizione. A tal uopo soccorre la dottrina che comunemente ha definito elementi essenziali e caratterizzanti la scrittura privata: il *documento*, la *dichiarazione*, la *sottoscrizione*⁷⁸, la *provenienza*⁷⁹. Appare opportuno qui sottolineare, dopo questa breve disamina circa la definizione giuridica di documento, che la dichiarazione contenuta nello stesso può palesarsi con

⁷⁶ IRTI, *Sul concetto giuridico di documento*, cit.

⁷⁷ Distinguibile a sua volta tra forma richiesta *ad substantiam* (art. 1325 n.4 c.c. et art. 1350 c.c.) e forma richiesta *ad probationem*. Si sottolinea che la forma *ad probationem* non incide sulla validità (*rectius*: esistenza) del contratto ma solo sui mezzi a disposizione per provarlo (cfr. artt. 2721-2739 c.c.). Sul piano stragiudiziale, al di fuori della lite, la differenza tra le due forme comporta che il contratto non stipulato per iscritto, per il quale sia però richiesta la forma *ad probationem*, è suscettibile di esecuzione, di accertamento e di ricognizione in quanto perfettamente valido ed efficace. Così GAZZONI, *Manuale dir. priv.*, IV ed., 1993, p. 865 ss.

⁷⁸ Circa l'essenzialità di questo requisito cfr. quanto riportato nel par. precedente.

⁷⁹ In quanto la scrittura deve essere formata da un privato, e non da un pubblico ufficiale nell'esercizio delle proprie funzioni. In questo senso C. BIANCA, G. PATTI, S. PATTI in *Lessico di diritto civile*, Giuffrè, 1991

qualsiasi forma di linguaggio, e quindi con *qualsiasi* combinazione di segni. Infatti, tanto la dottrina¹⁰ quanto la giurisprudenza¹¹, rilevano che nessuna norma di legge disciplina il tipo di linguaggio che occorre utilizzare per aversi scrittura privata: si è quindi sostenuto che anche il crittogramma¹², in quanto sottoscritto, sia scrittura privata astrattamente idonea ad essere oggetto di perizia per scoprirne la “chiave”.

I problemi affrontati dalla dottrina circa l'inquadramento giuridico del documento informatico¹³ sono essenzialmente i seguenti:

1. Se il documento informatico sia documento anche in senso giuridico.
2. Se, una volta data soluzione positiva al problema di cui sopra, possa ritenersi il documento informatico un documento scritto, ovvero, *mutatis mutandis*, possa postularsi l'equazione “forma elettronica = forma scritta”.

¹⁰ Cfr. MARMOCCHI, *Scrittura privata*, in Riv. not., 1987, p. 967; DI SABATO, *Il documento contrattuale*, cit.

¹¹ App. Perugia 3 dicembre 1952, in Giust. Civ., 1953, p.666.

¹² Da *Crittografia* che significa “scrittura cifrata o convenzionale, che non può essere compresa se non da chi ne conosca la chiave”. Definizione tratta da DIZIONARIO GARZANTI DELLA LINGUA ITALIANA, ult. ed.

¹³ La dottrina distingue tra *documento elettronico in senso stretto*, intendendosi con questa formula il documento formato dall'elaboratore elettronico, memorizzato in forma digitale (come sequenza di numeri binari), contenuto nella memoria centrale dell'elaboratore o nelle c.d. memorie di massa (principalmente supporti magnetici, tipo floppy-disk, ed ottici, tipo compact-disc) e leggibile solamente dalla macchina e non dall'uomo, se non tramite la macchina e *documento elettronico in senso ampio*, intendendosi con questa formula, tutti quei documenti formati dall'elaboratore mediante i propri organi di uscita (c.d. periferiche), quali potrebbero essere, ad esempio, i tabulati meccanografici. Ovviamente i problemi riscontrati dalla dottrina in ordine alla natura giuridica del documento elettronico, di cui si tratta in questo paragrafo, riguardano la prima delle due categorie sopra riportate, potendo infatti i c.d. documenti elettronici in senso ampio essere sottoscritti in maniera tradizionale e non ponendo conseguentemente problemi in ordine alla loro paternità e integrità. In tal senso E. GIANNANTONIO, *Manuale di diritto dell'informatica*, 1994, p.338 ss. richiamato da R. ZAGAMI, *Firme digitali, crittografia e validità del documento informatico*, in Riv. dir. inf., 1996, p.153.

3. Se siano riconducibili al documento informatico gli effetti sostanziali e probatori tipici della scrittura privata.

Per quanto riguarda i problemi *sub* 1.e *sub*.2, è opinione ormai pacifica in dottrina¹⁴ che il documento elettronico possa considerarsi documento in senso giuridico e soprattutto documento scritto. Questa conclusione risulta agevole ove si consideri che il *supporto informatico*, al pari del documento tradizionale (cartaceo), è dotato del requisito della materialità¹⁵ ed è parimenti idoneo a svolgere quella “funzione rappresentativa di un fatto” che abbiamo visto essere, rispettivamente, i requisiti essenziali per potersi parlare di documento in senso giuridico. Per quanto concerne la c.d. forma elettronica, essa è sicuramente sussumibile nel concetto di forma scritta: abbiamo infatti visto che la dichiarazione contenuta nel documento può palesarsi con qualsiasi forma di linguaggio, e quindi con qualsiasi

¹⁴ Fra i tanti che si sono occupati dell'argomento: ORLANDI, *La paternità delle scritture*, 1997; R. ZAGAMI, *Firme digitali ecc.*, cit.; DEL VECCHIO, *Riflessioni sul valore ecc.*, cit.; GIANNANTONIO, *Manuale ecc.*, cit. e anche dello stesso A., *Il valore giuridico del documento elettronico*, in Riv. dir. comm., 1986, I, p. 261 ss.; PAOLUCCI - FERRARESE, *Il documento informatico è documento giuridico*, in Federnotizie, 1990, p.23; BORRUSO, *Tre tesi di fondo dell'informatica giuridica*, in Giur. it., 1986, IV, p.219 ss.; STALLONE, *La forma dell'atto giuridico elettronico*, in Contratto e impresa, 1990

¹⁵ Ovviamente ciò dipenderà dal tipo di supporto informatico utilizzato in concreto. Si possono distinguere varie tipologie di supporto informatico (da intendersi come “qualsiasi materiale idoneo ad ospitare la registrazione in bit dei dati, ad uso del computer, al quale viene dato il nome di memoria”):

— *Supporti ottici* (compact-disc), in cui i dati vengono registrati mediante incisione a mezzo raggi laser. Detti supporti non sono riscrivibili e quindi sono idonei a rivelare alterazioni successive.

— *Supporti magnetici* (floppy-disks, hard-disks), ove la registrazione avviene mediante magnetizzazione o smagnetizzazione di determinate parti del supporto. Non sono in grado di rendere i dati immessi assolutamente intangibili, in quanto gli stessi possono sempre essere modificati o eliminati in qualsiasi momento mediante facili e semplicissimi comandi, senza lasciare traccia della precedente registrazione.

— *Supporti elettronici* (in senso stretto), ove la registrazione dei dati avviene attraverso il passaggio del flusso degli elettroni attraverso appositi apparati meccanici.

combinazione di segni. È stato, infatti, efficacemente detto¹⁶ che “tramite il computer, il flusso di elettroni è diventato il *nuovo* inchiostro dell’umanità (...), le memorie elettroniche sono la nuova carta, cioè il *nuovo* supporto su cui scrivere, i bit il *nuovo* alfabeto”: affermazione, questa, più che legittima considerando che inalterata rimane la funzione caratterizzante del documento, e cioè la trasmissione di informazioni, pur modificando il tipo di supporto incorporante queste ultime.

Sulla base di queste considerazioni riesce abbastanza agevole superare alcune obiezioni avanzate da altra parte della dottrina.

Da un lato, quelle di chi¹⁷ considera la forma elettronica come un *tertium-genus* rispetto alla forma scritta e a quella verbale, in base alla considerazione che il nostro codice, almeno fino alla L. n°59/97, conoscendo solo queste due modalità di trasmissione delle informazioni, ammette solo un’interpretazione evolutiva delle medesime, talché *tertium non datur*.

Dall’altro, negare validità alla tesi di chi¹⁸ sostiene come inesistente la forma elettronica, in base all’assunto che questa non sarebbe dotata degli attributi della forma scritta, in particolare di quello della immediata leggibilità-intelleggibilità (quale garanzia del principio di certezza del traffico giuridico), in ciò rivelandosi inidonea ad essere sussunta in quest’ultima.

¹⁶ Così BORRUSO, *Tre tesi di fondo dell’informatica giuridica*, cit. e così anche la dottrina maggioritaria, tra cui GIANNANTONIO, *Manuale ecc.*, cit.; DEL VECCHIO, *Riflessioni ecc.*, cit. ecc.

¹⁷ CLARIZIA, *Informatica e conclusione del contratto*, 1985, p.100

¹⁸ STALLONE, *La forma dell’atto giuridico elettronico*, cit., p.756 ss.

Infatti, la memoria elettronica “è già *in sé* un testo intelleggibile, giacché può essere letto attraverso la decodificazione binaria operata tramite computer: che il nudo senso umano sia insufficiente alla lettura del testo non muta punto la natura del fenomeno, perché non esiste una modalità tipica ed esclusiva della percezione sensoriale. L'osservante sarà chiamato ad utilizzare la macchina informatica alla stregua di una lente di ingrandimento”¹⁹.

Di più difficile soluzione è stata, per la dottrina, la soluzione del problema di cui al punto 3, e cioè se si potessero attribuire al documento informatico gli effetti sostanziali e probatori propri della scrittura privata. Se, infatti, si richiama alla mente la distinzione, più sopra riportata, fra documento elettronico in senso ampio e documento elettronico in senso stretto, ne deriva questa conseguenza: che, accanto a utilizzazioni dell'elaboratore nell'ambito del commercio giuridico volte alla creazione di una qualche risultanza documentale, si affiancano le ipotesi in cui l'impiego del computer non è direttamente finalizzato o tecnicamente volto ad ottenere un documento, ma semplicemente a “colloquiare” con uno o più elaboratori attraverso reti telematiche.

In tal caso il computer può giocare un ruolo importante nel processo di formazione del contratto, nel senso che attraverso di esso possono dipartirsi proposte ed accettazioni contrattuali, ordini di forniture e di acquisto di titoli, ecc.

¹⁹ In questi termini ORLANDI, *La paternità delle scritture*, cit., p.501. A sostegno di quanto riportato nel testo, si veda quanto più sopra riportato circa la validità come scrittura privata di un

Il computer diventa, in altre parole, ora lo “strumento che incide direttamente nel processo di formazione della volontà contrattuale”, ora il “luogo di incontro di volontà già perfezionatesi”²⁰.

In questo contesto è sorto il problema di stabilire quali effetti sostanziali e probatori riconoscersi agli elaborati informatici, alcuni dei quali si presentano sotto la forma di testi scritti (ma il più delle volte memorizzati su supporti magnetici, tipo floppy disk, che come abbiamo visto non offrono alcuna garanzia circa la verificabilità di alterazioni successive al testo originario), ma non sottoscritti.

Ci si chiedeva, quindi, quale rilevanza avesse il documento elettronico in relazione agli aspetti formali dell'attività negoziale. Ebbene, nel caso di contratti a forma libera, non c'è dubbio che la stipula possa avvenire tramite la posta elettronica (c.d. *e-mail*): trattandosi, infatti, di negozi in cui la dichiarazione può manifestarsi in qualunque modo, non può non riconoscersi validità a questo modo di comunicazione della volontà negoziale.

Le cose, però, si complicano allorché si tratti di stipulare contratti per i quali è prevista una forma *ad substantiam* (art. 1325 n. 4, art. 1350 c.c.), sia nel senso primo dell'espressione, cioè di forma condizionante il perfezionamento del negozio, sia nel senso diverso concernente la mera producibilità di effetti ulteriori rispetto ad esso (ad esempio l'opponibilità a terzi o altro). Il fatto che i soggetti dell'economia moderna comunichino, piuttosto che con lettere

testo crittografato.

²⁰ Così PARISI, *Il contratto concluso mediante computer*, 1987, p. 4 ss.

firmate dal mittente, attraverso segnali trasmessi da apparati meccanici, ha ridotto, infatti, il ricorso alla firma autografa quale criterio di assunzione della paternità del documento e rende ragione a chi²¹ parla del fenomeno come “crisi della sottoscrizione”.

In particolare ci si domandava se il documento elettronico, in cui si sostanzia lo scambio di dichiarazione contrattuale tramite computer, potesse valere come scrittura privata, essendo pacifico che, prima della legge n. 59 del 1997, non potesse valere né come scrittura privata autenticata né come atto pubblico (art. 2699 c.c.), per il quale è richiesto l'intervento di un pubblico ufficiale, terzo rispetto alle parti.

Abbiamo visto che fra i requisiti richiesti perché si possa parlare di scrittura privata figurava la sottoscrizione. Rimando al paragrafo precedente per le considerazioni relative alla (presunta) necessità di questo strumento come mezzo per assicurare quella che ho chiamato funzione di “imputabilità”.

Ciò che importa rilevare è che:

1. La provenienza della dichiarazione da una certa macchina non comporta necessariamente la provenienza da una certa persona;
2. La sicurezza della firma (o comunque di altre soluzioni, diverse dalla sottoscrizione tradizionale, idonee a garantire la funzione di imputabilità) attuata con mezzi non codificati esiste solo in quanto detti mezzi siano applicati al caso concreto; cioè, mentre la sottoscrizione autografa realizza le sue funzioni sempre e comunque, il documento elettronico è

²¹ IRTI, *Idola libertatis*, 1985, p. 75 e ZAGAMI, *Firme digitali ecc.*, cit., p. 152.

pure in grado di realizzarle, ma solo in astratto o, meglio, solo se gli utilizzatori applicano determinati standard tecnici (arg. *ex art.* 1352 c.c. “*Se le parti hanno convenuto per iscritto di adottare una determinata forma per la futura conclusione di un contratto, si presume che la forma sia stata voluta per la validità di questo*”).

E' pur vero che esistono supporti informatici, diversi da quelli magnetici, in grado di garantire l'inalterabilità del documento originale (le c.d. memorie informatiche WORM, lett.: *Write Once Read Many*) e che ci sono sistemi di identificazione per dati biometrici (impronte digitali, esame della retina, riconoscimento vocale ecc.) i quali, analizzati dal computer, sono in grado di identificare la persona umana in modo certamente più preciso della sottoscrizione tradizionale, di modo che pare lecito parlare di *nuovi metodi di imputazione* che fanno leva *non* sul legame fisico tra autore della dichiarazione e documento (come avveniva per il tramite della sottoscrizione autografa), ma su quella che efficacemente è stata definita “*esclusività dell'apparato tecnico*”²². Ma rimane comunque il fatto, come peraltro rilevato dalla dottrina più attenta²³, che in mancanza di una norma specifica disciplinante gli effetti sostanziali del documento elettronico, questo non possa essere considerato scrittura privata e questo perché il documento elettronico è suscettibile di realizzare la tutela delle esigenze, cui sopperiva la

²² Così IRTI, *Il contratto tra “facendum” e “factum”*, in Studi sul formalismo negoziale, 1997, p. 135.

²³ Così ZAGAMI, *Firme ecc.*, cit.; GIANNANTONIO, *Manuale*, cit.; VERDE, *Per la chiarezza di idee in tema di documentazione informatica*, in Riv. dir. proc., 1990, p. 721.

sottoscrizione tradizionale, *solo* in presenza di certi standard tecnici, che possono esserci come non esserci negli elaboratori utilizzati dalle parti contrattuali. Pertanto, come rileva efficacemente Zagami²⁴, “il documento elettronico in sé considerato, presenta una congenita impossibilità di verifica della sua integrità”, di modo che “non si possono immediatamente realizzare (...) quelle che sono state individuate come le funzioni proprie della sottoscrizione: funzione indicativa, funzione dichiarativa e funzione probatoria”²⁵.

Per quanto riguarda gli effetti probatori riconducibili al documento elettronico, stante l'impossibilità di applicazione della disciplina di cui agli artt. 2702 ss. c.c., gli interpreti²⁶ hanno inquadrato il fenomeno nel contesto delle prove documentali di cui all'art. 2712 c.c., che, riferendosi ad ogni rappresentazione meccanica di fatti e di cose, consente di disciplinare l'efficacia probatoria dei documenti prodotti da qualsiasi strumento meccanico, al quale può quindi equipararsi il documento informatico.

Le conseguenze processuali derivanti dall'applicazione dell'art. 2712 c.c. sono essenzialmente due:

— Il documento fa piena prova, in mancanza di disconoscimento, dei fatti in esso rappresentati e quindi il giudice è obbligato a ritenere provato il fatto

²⁴ ZAGAMI, *Firme ecc.*, cit., 1996.

²⁵ Queste difficoltà, dopo l'emanazione della l. 59/97, e, in particolare dell'art. 5 del D.P.R. 513 del 1997, sono state superate grazie all'adozione, da parte del legislatore italiano, delle tecniche di crittografia asimmetrica che, mediante l'apposizione di firme digitali, sono in grado di garantire tanto la paternità quanto l'integrità del documento informatico.

²⁶ GIANNANTONIO, *Manuale*, cit.

rappresentato. La differenza rispetto alla scrittura privata, sta nel fatto che questa efficacia ha natura endoprocessuale, anziché essere *erga omnes*.

— L'onere di disconoscimento gravante sulla parte contro cui viene prodotto il documento non è sottoposto ai termini di cui all'art. 215 c.p.c. e ad esso non è applicabile il procedimento di verifica di cui agli artt. 216 ss. c.p.c.²⁷.

3. CRITTOGRAFIA SIMMETRICA E ASIMMETRICA

Abbiamo visto al paragrafo precedente che la difficoltà maggiore nell'attribuire al documento informatico l'efficacia di scrittura privata era dovuta, da un lato, all'impossibilità di sottoscriverlo nei modi tradizionali, e, dall'altro, anche ritenendo superabile questo ostacolo, avvalendosi dei progressi delle scienze informatiche¹ e dei sistemi di identificazione dei dati biometrici, rimaneva comunque il fatto che, in assenza di una disciplina normativa che regolasse la materia e nello specifico gli effetti sostanziali e

²⁷ Così MONTESANO, *Sul documento informatico come rappresentazione meccanica della prova civile*, in Riv. trim. dir. proc. civ., 1987.

probatori del documento elettronico, questo non potesse, comunque, essere considerato scrittura privata. Questa ulteriore preclusione discendeva dalla constatazione che il documento elettronico è suscettibile di realizzare la tutela delle esigenze, cui sopperiva la sottoscrizione tradizionale, *solo* in presenza di certi standard tecnici, che possono esserci come non esserci negli elaboratori delle parti contrattuali.

Ciò che in sostanza veniva meno, era la *certezza nei traffici commerciali*: mancando un riconoscimento a livello legislativo del fenomeno, le uniche norme invocabili per riconoscere piena validità al documento informatico, con un'efficacia peraltro limitata alle parti contraenti, erano l'art.1352 c.c.(rubricato "forme convenzionali": ne derivava l'applicabilità dell'art. 2725 primo comma c.c. che limita il ricorso alla prova testimoniale) per quanto riguarda l'aspetto formale, e l'art. 2698 c.c. per quanto riguarda l'aspetto probatorio (infatti, un accordo scritto sulla base dell'art. 1352 c.c., avrebbe prodotto un'inversione convenzionale dell'onere della prova).

In particolare, i problemi di ordine tecnico e giuridico stavano in ciò: che il documento tradizionale in forma cartacea è costituito da un *supporto*, ossia da un elemento materiale, da un "*mezzo*" – generalmente la scrittura – e da un *contenuto*, ossia dalla rappresentazione di un concetto²¹. La sua prerogativa

²¹ Mi riferisco al software P.G.P., realizzato da Philip Zimmermann negli Stati Uniti e diffuso in rete come freeware nel 1991, che è il programma di crittografia a chiavi asimmetriche più conosciuto in Internet.

²² È possibile, infatti, distinguere tra elemento materiale del documento (il supporto-contenente) ed elemento spirituale o intellettuale (il suo contenuto). Il primo è il mezzo nel quale è incorporata la scritturazione; il secondo è il pensiero materializzato nello scritto. In questo senso A. MORELLO, *Sottoscrizione*, in Nov. Dig. It., XVII, Torino, p.1004.

è quella di garantire l'autenticità e non modificabilità del contenuto. Questo è possibile in quanto esso costituisce un tutto unico con il contenente.

L'apposizione di una firma o di una qualsiasi certificazione (timbri, sigilli ecc.) si riferiscono sempre al contenente, al supporto, marchiandolo in modo non cancellabile e di conseguenza anche al contenuto, talché sarebbe impossibile pensare, pena la perdita di ogni rilevanza giuridica, a una scissione tra contenuto e contenente.

Un *file* di testo (o un qualunque file digitale) non costituisce di per sé un documento (informatico) equivalente in tutto e per tutto a quello cartaceo, in quanto esso può essere modificato o riprodotto infinite volte³³ senza alcuna difficoltà e non fornisce alcuna garanzia di provenienza. Il contenuto è totalmente svincolato dal contenente (si parla a tal proposito di *immaterialità del documento elettronico*): un numero potenzialmente infinito di "copie" può essere agevolmente trasferito su un supporto diverso (ad esempio da un supporto ottico a uno magnetico e viceversa); le "copie" saranno in tutto e per tutto *identiche agli originali*, mentre ciò non accade con i documenti tradizionali³⁴.

³³ Ho accennato al paragrafo precedente che l'inalterabilità del supporto potrebbe essere garantita dall'utilizzo di supporti ottici (tipo cd-rom worm), perché non riscrivibili. Qui aggiungo, però, che tale risultato, se da un lato crea lo stesso legame fisico tra contenente e contenuto proprio dei tradizionali supporti cartacei – difettando comunque la garanzia derivante dall'immutabilità del contenuto al suo autore – ne presenta anche gli stessi limiti (impossibilità di scindere il contenuto dal contenente, pena la perdita di efficacia giuridica), di fatto inconciliabili con il moderno sistema delle transazioni on-line. Si pensi, ad esempio, all'invio di una proposta contrattuale per posta elettronica.

³⁴ Infatti la copia di un documento cartaceo (passaggio del contenuto da un contenente ad altro contenente) richiede idonee garanzie perché conservi la stessa efficacia probatoria (artt. 2714 – 2719 c.c.).

Si rende quindi necessario un *tipo di autenticazione*, come quella garantita dalla firma digitale, *che si riferisca non al contenente ma al contenuto stesso*.

La firma digitale⁵⁵, che la dottrina ha definito come “un’insieme di caratteri alfanumerici risultante da complesse operazioni matematiche di crittografia effettuate da un elaboratore su un documento elettronico”⁶⁶, può quindi trasformare una sequenza di *bit* privi di rilevanza giuridica, se non in base ad accordi contrattuali tra le parti e validi solo per le parti stesse, in un vero e proprio documento informatico a cui la normativa italiana, a determinate condizioni⁷⁷, attribuisce la stessa validità del documento su supporto cartaceo.

Il D.P.R. 513/97 e il successivo D.P.C.M. 8 febbraio 1999 dando attuazione all’art. 15 della L.59/97 hanno privilegiato un sistema di firma digitale basato sulla c.d. crittografia “a chiave pubblica”.

La crittografia (dal greco *crypto* = “nascondere” e *graphein* = “scrivere”) è una scienza matematica che serve, principalmente a cifrare un testo (si pensi sempre alla solita proposta contrattuale contenuta in una *e-mail*) in modo da renderlo assolutamente incomprensibile, se non al destinatario, assicurando

⁵⁵ Il D.P.R. 513/97 all’art. 1 lett. b) definisce la firma digitale come “ il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente di rendere manifesta e si verificare la provenienza e l’integrità di un documento informatico o di un insieme di documenti informatici”. Viene data anche la definizione di sistema di validazione (cioè il software di crittografia), da intendersi come “il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità” (art. 1 lett. c)).

⁶⁶ Così R. ZAGAMI, in *Firme digitali...ecc*, cit. Vedi anche L.G. LAWRENCE, *Digital signatures – explanation and usage*, in *Computer & Security*, 1993, p.230 ss.; S. GARFINKEL, *P.G.P. Pretty good privacy*, O’ Reilly, U.S.A., 1995.

così una funzione di segretezza⁷⁸; inoltre, adottando un sistema di crittografia a chiave pubblica è anche possibile garantire l'autenticità e la integrità del testo cifrato.

La crittografia si basa essenzialmente sull'applicazione, al testo da cifrare, di una funzione matematica (c.d. *algoritmo di codifica*⁷⁹) azionabile mediante un apposito codice (c.d. *chiave*). L'algoritmo di codifica è una *funzione reversibile*: ne deriva che l'applicazione *a contrario* dello stesso algoritmo e della chiave (e qui, ovviamente, sarà necessario distinguere fra il tipo di chiavi a seconda del tipo di sistema crittografico, in concreto, utilizzato) permette di rendere di nuovo leggibile il testo originario.

Le tecniche di crittografia sono suddivisibili, principalmente, in due categorie:

- Crittografia *simmetrica*, o a “chiave privata”, basata sull'utilizzazione di un'unica chiave sia per cifrare che per decifrare il testo.
- Crittografia *asimmetrica*, o a “chiave pubblica”, basata sull'utilizzazione di una coppia di chiavi (una privata e l'altra pubblica), fra di loro in

⁷⁸ Cfr. l'art. 5 del D.P.R. 513/97 et *amplius* vedi cap. II, par. 2 e seguenti.

⁷⁸ Viene così assicurato quel diritto alla libertà e segretezza della corrispondenza (le *e-mail*, altro non sono che lettere digitali), garantito dall'art. 15 Cost., limitabile solamente per comprovate esigenze di tutela dell'ordine pubblico.

⁷⁹ L'algoritmo di codifica più utilizzato in ambito di crittografia simmetrica è il *Data Encryption Standard* (DES), inventato da alcuni ricercatori dell'IBM e poi adottato come standard dalle agenzie federali degli Stati Uniti verso la metà degli anni settanta. L'algoritmo di codifica più utilizzato in ambito di crittografia asimmetrica è l'R.S.A. (riconosciuto come standard dal nostro legislatore, unitamente all'algoritmo DSA: cfr. art. 2 del D.P.C.M. 8 febbraio 1999). Prende il nome dalle iniziali dei cognomi dei suoi autori (Rivest, Shamir, Adleman), ricercatori al Massachusetts Institute of Technology, che lo svilupparono nel 1977. Cfr. G. ROGNETTA, *La firma digitale e il documento informatico*, Ed. Simone, 1999.

relazione biunivoca¹⁰. L'una viene utilizzata per cifrare il testo e l'altra per decifrare il medesimo. In altri termini, il documento codificato con una delle due chiavi può essere decodificato solo con l'altra chiave, e non riutilizzando la prima (c.d. *complementarità* delle chiavi).

La scelta del legislatore italiano è caduta sulla seconda delle categorie sopra menzionate¹¹, perché l'utilizzazione di un sistema di crittografia simmetrica non avrebbe soddisfatto quel principio di *certezza del diritto* che doveva (e deve!) caratterizzare le operazioni negoziali del commercio "virtuale", al pari delle operazioni contrattuali concluse mediante strumenti tradizionali.

In particolare, per quanto riguarda l'ambito contrattuale (e specificatamente il momento perfezionativo), un sistema di crittografia simmetrica si rivela idoneo a tutelare, al più, l'esigenza di *riservatezza* dei dati; inidoneo, invece, a tutelare la non contraffazione dei medesimi (*integrità*), a dimostrare la provenienza delle informazioni (*autenticità*), nonché a garantire la *non ripudiabilità* (chi trasmette/riceve, ad es. una proposta contrattuale, non può negare di aver trasmesso/ricevuto).

Infatti, l'utilizzazione di un'unica chiave tanto per cifrare quanto per decifrare il testo può esporre a questo pericolo: che, in fase di formazione di

¹⁰ Biunivocità è termine che indica la corrispondenza secondo cui ad ogni elemento di un insieme corrisponde uno ed un solo elemento di un altro insieme e viceversa. Cioè per ogni chiave privata è impossibile aversi due chiavi pubbliche identiche e viceversa.

¹¹ Con tutti i correttivi del caso: mi riferisco al sistema di certificazione "verticale" delle chiavi pubbliche affidato ad apposite società di certificazione (in possesso di particolari requisiti relativamente alla loro struttura e alle modalità di esercizio della loro attività: cfr., rispettivamente, gli artt. 8-9 del D.P.R. 513/97 e il D.P.C.M. 8 febbraio 1999), in luogo di quello "orizzontale" utilizzato diffusamente in internet da parte degli utenti del software P.G.P.

un accordo contrattuale – ad esempio -, Caio, accettante, dopo aver decifrato con l'apposita chiave il messaggio contenente la proposta di Tizio, la modifichi a suo piacimento prima dell'accettazione e sostenga poi la provenienza da Tizio. È ovvio che questa si configurerebbe come una soluzione inaccettabile sul piano della certezza del diritto.

A ciò si aggiunga che dovrebbero generarsi tante chiavi quante potrebbero essere le coppie contrattuali (proponente/accettante) potenziali utilizzatrici del sistema, e che, in difetto di un canale sicuro di trasmissione della chiave (e tale non può essere considerata, senza ulteriori accorgimenti tecnici, la rete telematica), si paleserebbe la necessità di un incontro fisico fra le due parti per concordare il codice comune. Eventualità, quest'ultima, di certo “non in linea” con un sistema che dovrebbe funzionare anche fra interlocutori separati da grandissime distanze.

A questi inconvenienti sopperisce un sistema di crittografia¹² (o “sistema di validazione”, secondo la definizione datane dall'art.1 lett. c) del D.P.R. 513/97), a chiavi asimmetriche, perché le firme digitali contribuiscono¹³ a tutelare la riservatezza, l'integrità, l'autenticità, nonché a garantire (attraverso

¹² Cfr. L. FELICIAN, *Crittografia: istruzioni per l'utilizzo*, in “Il sole 24 ore” del 13 febbraio 1998.

¹³ Non si può, ovviamente, ottenere la certezza matematica, valida *semper et semper*, della c.d. inviolabilità di un sistema informatico. In riferimento a chiavi asimmetriche del tipo adottato dal nostro legislatore (in base all'algoritmo RSA la lunghezza delle chiavi può essere di 384, 512, 1024 bit), è stato calcolato che “una rete di un milione di computer impiegherebbe un tempo corrispondente all'età dell'Universo per ricavare una chiave privata da una chiave pubblica. Questo non esclude che in futuro si possa violare ciò che oggi appare inviolabile: ciò che conta, però, è che, allo stato delle attuali conoscenze tecniche, il sistema sia completamente affidabile”. Così G. ROGNETTA, *La firma digitale e il documento informatico*, cit., p.10 nota 7.

un apposito sistema di certificazione delle c.d. “*public keys*”) la non ripudiabilità dei contenuti di un documento informatico.

Infatti, a differenza del sistema tradizionale simmetrico, il sistema a chiavi asimmetriche consta di due chiavi di cifratura attribuite a *ogni* utilizzatore: denominate “privata” l’una, in uso esclusivo del soggetto titolare, e “pubblica”, quella destinata, appunto, a essere pubblicata in appositi registri on-line (c.d. *key repositories*), accessibili a chiunque.

Prenderemo ora in considerazione le possibili applicazioni della crittografia a chiave pubblica, non senza aver, però, sottolineato nuovamente che condizioni essenziali per il corretto funzionamento (anche giuridico!!) del sistema sono:

- La chiave privata deve essere conosciuta *solo* dal soggetto titolare di essa (art. 1 lett. e) del D.P.R. 513/97)^{14□}.
- La conoscenza della chiave pubblica non deve permettere di risalire alla chiave privata (c.d. *indipendenza* delle chiavi), in esclusiva disponibilità quest’ultima, del soggetto titolare.

La *funzione di segretezza* del documento è assicurata cifrando il testo in oggetto con la chiave pubblica del destinatario. Il destinatario userà la propria chiave privata (corrispondente a quella pubblica utilizzata dal mittente) per

^{14□} E, secondo quanto disposto dall’art. 9, primo comma, del D.P.R. 513/97, deve rimanere nella sua esclusiva disponibilità, di modo che un uso illegittimo della chiave configurerebbe un caso di responsabilità oggettiva per danno a terzi nel caso che il titolare non “adotti tutte le misure organizzative e tecniche idonee ad evitare danno ad altri”. Vedi *amplius* Cap. II, par.4

decifrarlo. È importante notare che, data la biunivocità delle chiavi, solo il destinatario, e nessun altro, potrà decifrare il documento (fig. 1).

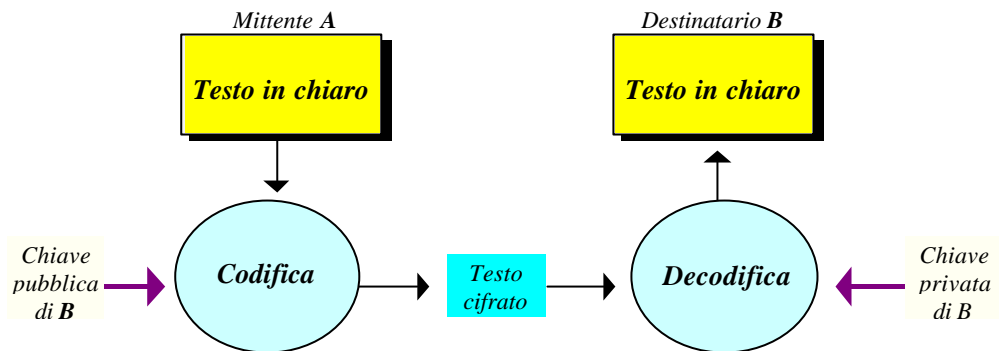


Figura 1 - La tecnica di protezione della riservatezza attraverso la crittografia a chiave pubblica

Tramite questa prima applicazione del sistema non viene però garantita né l'integrità né la provenienza del documento, perché chiunque potrebbe impossessarsi della chiave pubblica del destinatario e inviargli un documento cifrato, nel caso una proposta contrattuale via *e-mail*, attribuendosi un falso nome o spendendo, illegittimamente, un nome altrui.

L'autenticità del documento e la sua integrità vengono assicurate mediante la seconda delle possibili applicazioni della crittografia asimmetrica, ed è in tale applicazione che si genera la firma digitale. Infatti, "una firma digitale è il risultato dell'applicazione di una chiave privata ad un documento informatico. Chiunque voglia verificare la sua autenticità applicherà la chiave pubblica corrispondente e potrà essere certo, da un lato, della provenienza del documento da parte di una persona che ha la disponibilità della chiave

privata; dall'altro, *dell'integrità* dello stesso al momento dell'applicazione della firma digitale"¹⁵ (fig.2).

La firma digitale può essere applicata tanto all'intero documento quanto ad un estratto di esso (il c.d. *message digest* o *hash code*, ottenuto tramite l'applicazione al documento informatico una particolare funzione matematica, la c.d. *funzione di hash*)¹⁶. Il risultato (visivo) che si ottiene è il seguente: un insieme incomprensibile di dati alfanumerici sostitutivi dell'intero documento, nel primo caso; sostitutivi di una parte, solamente, dello stesso nel secondo.

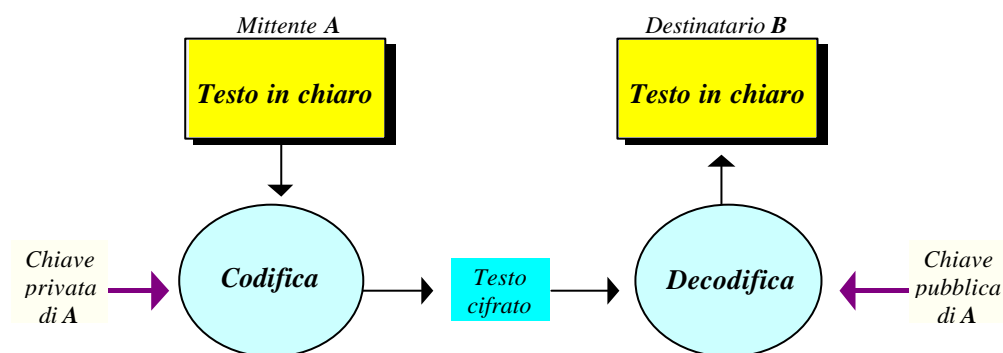


Figura 2 - La tecnica di autenticazione attraverso la crittografia a chiave pubblica

¹⁵ Così R. ZAGAMI, *Firme digitali...ecc.*, cit.

¹⁶ La firma digitale può, quindi, essere di due tipi:

— *Firma con ricostruzione del messaggio*: il messaggio coincide con la firma digitale. Nel momento stesso in cui il destinatario verifica la firma digitale, con l'applicazione al documento-firma della chiave pubblica corrispondente, rende anche leggibile *in toto* il documento e contestualmente ottiene una verifica (positiva) circa la sua integrità.

— *Firma con appendice*: La firma è calcolata su una sorta di "riassunto" del documento (c.d. *message digest*). Viene quindi allegata al documento *in chiaro* e spedita al destinatario che ne verifica l'integrità.

Di contro questa seconda applicazione non tutela la riservatezza, atteso che chiunque dispone del documento può leggerlo, applicando la chiave pubblica del “sottoscrittore”, prelevata on-line dai c.d. *key repositories*. Combinando, però, le due applicazioni, sopra esemplificate, si riesce ad assicurare nel contempo, la riservatezza del contenuto dei dati, l'autenticità e l'integrità degli stessi (fig. 4). Qualora, infatti, il mittente utilizzi la propria chiave privata per firmare digitalmente il documento e quella pubblica del destinatario per cifrarlo, quest'ultimo lo decifrerà utilizzando la propria chiave privata (ottenendo, terminata questa prima operazione, un testo ancora cifrato, essendo quest'ultimo il risultato dell'apposizione della firma digitale “all'origine”) e ne verificherà l'autenticità e l'integrità, usando la chiave pubblica del mittente (ottenendo, terminata questa seconda operazione e se la verifica da esito positivo, un testo perfettamente leggibile e comprensibile).

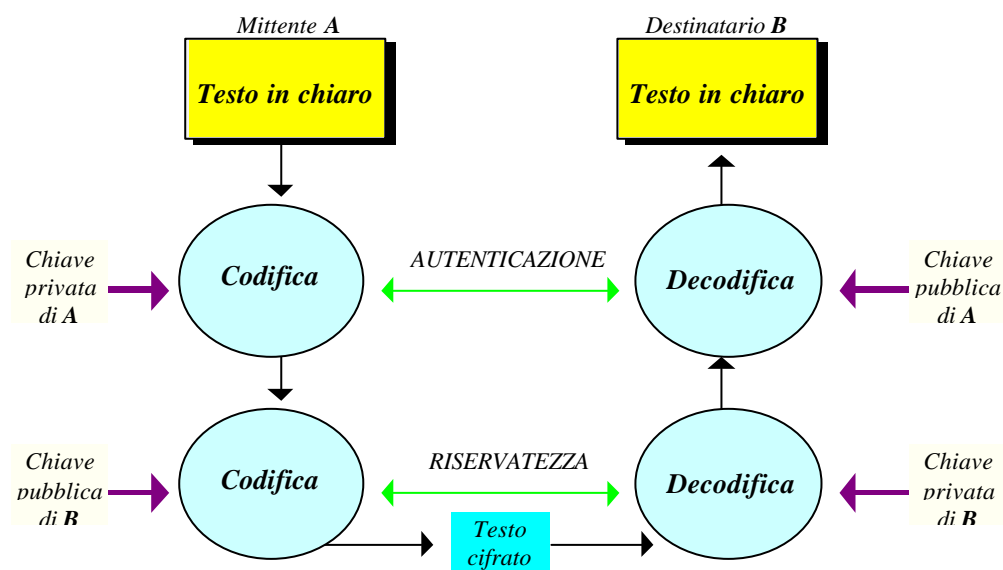


Figura 4 - Autenticazione e riservatezza attraverso la crittografia a chiave pubblica

A conclusione di questa breve disamina sul *come* funzioni il sistema di firma digitale, occorre un'ulteriore precisazione, indispensabile affinché la trattazione della materia in oggetto sia veramente esaustiva: abbiamo più sopra constatato che, risultato dell'applicazione della firma digitale a un documento elettronico è, da un lato, la possibilità di verifica dell'integrità del documento firmato e, dall'altro, la possibilità di accertamento della paternità dello stesso, nel senso che *a verifica positiva* corrisponde la certezza che *quel* documento è stato firmato dal *titolare* della chiave privata che ha generato *quella* firma.

In breve: viene in evidenza, nel sistema fin qui descritto, la mancanza di un'indicazione *certa* circa la reale identità del titolare della coppia di chiavi; mancanza che potrebbe permettere a chiunque di creare delle coppie di chiavi, associarle ad un nome di altra persona, pubblicare on-line la chiave pubblica e quindi usare il nome falso e la chiave privata corrispondente per generare firme digitali.

Ci si troverebbe di fronte ad un problema di *inattendibilità* dell'attribuzione delle chiavi pubbliche¹⁷, che non può permettersi, pena la perdita di ogni certezza giuridica.

¹⁷ È quello che succede con il diffusissimo programma di crittografia asimmetrica *Personal Good privacy* (PGP), il quale si basa in sostanza su un'attività di certificazione c.d. "orizzontale". Il PGP

Per questo il D.P.R. 513/97 all'art. 8 disciplina la figura dei certificatori: società per azioni, con un capitale sociale non inferiore a quello necessario per svolgere l'attività bancaria, in possesso di particolari requisiti gestionali, tecnici e organizzativi, la cui attività è monitorata costantemente dall'A.I.P.A. (Autorità per la Informatica della Pubblica Amministrazione)^{18□}.

La funzione principale cui queste società sono deputate è, appunto, l'attività di certificazione definita all'art. 1 lett. h) del D.P.R. 513/97 come “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 (...)*”.

Ad un accertamento *ex post* della provenienza oggettiva di un documento informatico, da intendersi come corrispondenza biunivoca fra un determinato documento informatico, non alterato successivamente alla sua creazione, e la chiave privata utilizzata per firmarlo, si affianca, così, un accertamento *ex ante* della provenienza soggettiva di una determinata coppia di chiavi. Viene così garantita la piena equiparabilità, dal punto di vista funzionale, tra sottoscrizione tradizionale e firma digitale.

non prevede l'esistenza di un'Autorità di Certificazione che garantisca la corrispondenza tra una coppia di chiavi e il suo titolare: il programma, infatti, consente a ogni utente di firmare, con la propria chiave privata, la chiave pubblica di un altro utente, rendendola così *valida*. In sostanza, un utente funge da potenziale certificatore per gli altri utenti.

4. FIRMA DIGITALE E SOTTOSCRIZIONE: ANALOGIE E DIFFERENZE SOSTANZIALI

Da quanto esposto nei paragrafi precedenti riesce abbastanza agevole individuare le differenze strutturali tra la firma tradizionale e quella digitale così come individuarne le analogie, essendo oramai pacifico che la seconda assicura, al pari della prima (e tenuto conto dei diversi supporti su cui esse operano), il rispetto di quella funzione di imputabilità, necessaria per garantire la riferibilità di un documento al suo autore; funzione che lo stesso

¹⁸ Vedi *infra* cap. II, par. 1.

legislatore considera prevalente rispetto al mezzo, di volta in volta, ritenuto più idoneo a garantire la funzione stessa (arg. ex art. 2705 c.c.).

Da un punto di vista semantico appare appropriato l'uso della locuzione "firma digitale", fatto dal nostro legislatore, per designare il risultato di una particolare procedura informatica (il c.d. *sistema di validazione*, come definito dall'art. 1 lett. c) D.P.R. 513/97) capace di garantire la riferibilità "univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata" (art. 10 comma 3, D.P.R. cit.).

Infatti, le precedenti definizioni, proposte e dalla dottrina (tra le tante ricordo: "sigillo informatico"¹, "firma elettronica"², "sottoscrizione elettronica"³, ecc.) e dall'A.I.P.A. (il c.d. "contrassegno elettronico"⁴) non sarebbero risultate idonee a descrivere compiutamente il fenomeno.

Così, appare corretta l'utilizzazione dell'attributo "digitale" in luogo di "elettronica", essendo la firma digitale la risultante di un'attività di digitazione che ha come prodotto un'*informazione* espressa nel linguaggio

¹ Tale definizione è stata formulata da D. GIAQUINTO e P. RAGOZZO in *Il sigillo informatico*, nella rivista *Notariato*, I, 1996, p.80 ss.

² Così F. CHIOMENTI, *Firme autografe e firme meccaniche sui titoli di credito... e ora firme elettroniche*, in *Giurisprudenza Commerciale*, I, 1998, p.725 ss.

³ Così B. DEL VECCHIO, in *Riflessioni sul valore giuridico della sottoscrizione elettronica*, cit.

⁴ La prima bozza di schema di disciplina di "atti e documenti in forma elettronica" fu completata dall'Autorità per l'Informatica della Pubblica Amministrazione (A.I.P.A.), grazie anche al contributo del Consiglio Nazionale del Notariato, nel settembre 1996. Successivamente alla emanazione della L. 59/97 e in attuazione dell'art. 15 della stessa, l'A.I.P.A. completò la seconda bozza, questa volta "Schema di regolamento su atti, documenti e contratti in forma elettronica", che fu trasmessa nel giugno del 1997 alla Presidenza del Consiglio dei Ministri. Questa seconda bozza, nel testo corretto dalla apposita commissione istituita in seno al Consiglio dei Ministri, terminò l'*iter* procedimentale, con l'approvazione delle competenti commissioni di Camera e Senato e del Consiglio di Stato, giungendo alla definitiva delibera del Governo in data 31 ottobre 1997. Infine, dopo il ritardo causato dalla registrazione della Corte dei Conti, si arrivava alla pubblicazione del D.P.R. 513/97 sulla Gazzetta Ufficiale del 13 marzo 1998 n. 60.

dei bit (tra l'altro la firma digitale, anche alla luce della recente proposta di direttiva elaborata in sede comunitaria, sta in un rapporto di specie a genere con le firme elettroniche)⁵⁵.

È preferibile l'uso del sostantivo "firma" in luogo di "contrassegno", perché la funzione cui è preordinata la firma digitale è la stessa svolta dalla tradizionale sottoscrizione (funzione di imputabilità); funzione che non è propria del semplice contrassegno.

Più difficile risulta accordare preferenza al sostantivo "firma" rispetto a "sigillo informatico", poiché, come rileva attenta dottrina (Ragozzo e Giaquinto⁵⁶), se la firma digitale svolge la stessa funzione cui la firma autografa è preordinata, manca però del requisito "fisico" di quest'ultima; l'utilizzo della chiave privata può infatti avvenire anche da parte di terzi, legittimamente autorizzati dal titolare.

Di quanto detto è data conferma dall'art. 11 comma 3 del D.P.C.M. 8 febbraio 1999, il quale dispone che il certificato relativo ad una coppia di chiavi di sottoscrizione, rilasciato dalle s.p.a. dotate dei requisiti di cui all'art. 8 del D.P.R. 513/97 (c.d. *certificatori*), può indicare, oltre al contenuto

⁵⁵ Vedi *amplius* cap. IV.

⁵⁶ D. GIAQUINTO e P. RAGOZZO, *Il sigillo informatico*, cit., richiamati da VERDIANA FEDELI, in *Documento informatico e firma digitale: valore giuridico ed efficacia probatoria alla luce del decreto del Presidente della Repubblica 10 novembre 1997, n. 513*, in Riv. dir. comm., I, 1998.

minimo⁷⁷ di ciascun certificato, anche le eventuali limitazioni nell'uso della coppia di chiavi nonché gli eventuali poteri di rappresentanza.

Così, la summenzionata dottrina ha affermato che, in conformità alla non inscindibilità alla persona fisica del titolare, può ritenersi che la coppia di chiavi realizzi a pieno il *pendant* informatico del sigillo⁷⁸.

L'obiezione appare facilmente superabile, considerando che le eventuali limitazioni nell'uso della coppia di chiavi così come l'indicazione di eventuali poteri rappresentativi, fanno parte del contenuto *eventuale* del certificato che si contrappone a quello minimo necessario, specificato

⁷⁷ Il D.P.C.M. 8 febbraio 1999 all'art. 4 dell'allegato tecnico, distingue tre tipologie di chiavi asimmetriche in relazione ai soggetti di diritto abilitate ad utilizzarle in relazione alla loro funzione:

— *Chiavi di sottoscrizione*, generate sia dal titolare (persona fisica o giuridica) sia dal certificatore, con cui si generano e si verificano le firme apposte o associate ai documenti.

— *Chiavi di certificazione*, generate esclusivamente dal certificatore, con cui si generano e si verificano le firme apposte ai certificati e alle loro liste di revoca (Certificate Revocation List: CRL) e sospensione (Certificate Suspension List: CSL).

— *Chiavi di marcatura temporale*, generate esclusivamente dal certificatore, destinate alla generazione e verifica delle marche temporali.

Ad ogni coppia di chiavi corrisponde un certificato, avente la funzione di identificare "fisicamente" ed in modo univoco il titolare della chiave privata, il cui contenuto minimo-necessario è così delineato dal 1° comma dell'art. 11 D.P.C.M. cit.:

Art. 11. Informazioni contenute nei certificati.- I certificati debbono contenere almeno le seguenti informazioni:

- a) Numero di serie del certificato.
- b) Ragione o denominazione sociale del certificatore.
- c) Codice identificativo del titolare presso il certificatore.
- d) Nome, cognome e data di nascita ovvero ragione sociale o denominazione sociale del titolare.
- e) Valore della chiave pubblica.
- f) Algoritmi di generazione e verifica utilizzabili.
- g) Inizio e fine del periodo di validità delle chiavi.
- h) Algoritmo di sottoscrizione del certificato.

Dal certificato deve potersi desumere in modo inequivocabile la tipologia delle chiavi.

dall'art. 11 comma 1 del D.P.C.M. 8 febbraio 1999, da un lato; che il legame fisico-somatico che lega la firma tradizionale al suo autore può trovare cittadinanza anche nel mondo informatico, là dove il lecito accesso al sistema di validazione venga garantito da appositi sistemi di identificazione biometrica⁹⁸, dall'altro.

A prescindere da queste ultime precisazioni, non si può, comunque, non considerare che nella locuzione “firma digitale” il concetto stesso di firma acquista un nuovo significato, che non può esistere da solo, ma esclusivamente con l'attributo che lo qualifica, e che, come tale, rifiuta ogni catalogazione terminologica tradizionale.

Nemmeno può correttamente parlarsi, infine, di sottoscrizione elettronica, perché nel documento informatico non vi può essere alcuna autografia di un nominativo (“-scrizione”), né tantomeno può essere apposta in calce (“sotto-“) al documento.

Operati questi *distinguo* terminologici, è dato riscontrare la piena equiparabilità, dal punto di vista funzionale, tra firma digitale e sottoscrizione tradizionale.

Infatti, la prima assolve in pieno le funzioni che Carnelutti¹⁰⁰ (e la dottrina che gli è seguita) riteneva essere imprescindibili della seconda.

⁹⁸ Così VERDIANA FEDELI, *Documento informatico...*, cit., p. 817.

⁹⁹ Il D.P.R. 513/97 all'art. 1 lett. g) definisce la “chiave biometrica” come “la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente”.

¹⁰⁰ F. CARNELUTTI, *Studi sulla sottoscrizione*, cit., p. 509 ss.

Così, in relazione alla c.d. *funzione indicativa* (funzione di indicare l'autore di un documento), considerato che in ogni firma digitale è incluso un codice numerico identificante la chiave privata e la corrispondente chiave pubblica, e che proprio questo codice permette, in relazione alla chiave pubblica, di risalire al certificato identificante in maniera univoca il titolare della coppia di chiavi asimmetriche, si ritiene essa sia pienamente assolta. Lo stesso dicasi per la c.d. *funzione dichiarativa* (funzione di assumersi la paternità della dichiarazione di un documento), e così pure per la c.d. *funzione probatoria*, ottenibile mediante la combinazione di firma digitale e certificato, di guisa che si raggiunge la certezza che il documento proviene da una persona che ha la disponibilità della chiave privata corrispondente alla chiave pubblica certificata.

Passando ora ad analizzare quelli che la dottrina ha individuato essere i requisiti “ontologici”¹¹ della sottoscrizione tradizionale in relazione alla firma digitale, è di tutta evidenza come quest'ultima ne faccia propri alcuni, di altri faccia assoluto difetto, e altri ancora costituiscano attributi suoi propri:

- *Forma scritta.* È un requisito che la firma digitale possiede se si ritiene, come la maggior parte della dottrina¹² e ora per espresso riconoscimento legislativo (art. 4, comma 1, D.P.R. 513/97), il documento informatico essere documento scritto.

¹¹ F. CARNELUTTI, *Studi...*, cit.; A. MORELLO, *Sottoscrizione*, cit.; ORLANDI, *La paternità delle scritture*, cit. ecc.

¹² E. GIANNANTONIO, *Manuale di diritto dell'informatica*, cit.; DEL VECCHIO, *Riflessioni...*, cit.; BORRUSO, *Computer e diritto*, I, Milano, 1988, p.275.

- *Autografia.* È requisito che non è proprio della firma digitale.
- *Nominatività.* Questo requisito caratterizza la firma digitale ma con connotazioni del tutto particolari, talché si è parlato di “nominatività elettronica”¹³.
- *Leggibilità.* Secondo i più, è un requisito del tutto assente nella firma digitale, in quanto proprio nella mancanza di leggibilità risiede la garanzia della crittografia. A ben vedere però, ciò che difetta è il requisito della immediata leggibilità e non della leggibilità in sé considerata, in quanto questa sarebbe comunque ottenibile in sede giudiziale applicando la chiave pubblica corrispondente a quella privata che ha generato la firma¹⁴.
- *Riconoscibilità.* La firma digitale può dirsi dotata di questo requisito, dato che con l'applicazione della chiave pubblica corrispondente si compie quella verifica che, se positiva, assicura quella funzione probatoria cui il requisito di cui sopra è deputato.
- *Apposizione in calce al documento.* È requisito incompatibile con un sistema di firma digitale, venendo “applicata” quest'ultima sull'intero documento o su un estratto di esso¹⁵.
- *Non riutilizzabilità.* Quest'ultimo forse è il requisito che maggiormente caratterizza la firma digitale, avendo più sopra constatato che

¹³ Così DEL VECCHIO, *Riflessioni sul valore giuridico della sottoscrizione autografa*, cit.

¹⁴ Arg. ex. sentenza App. Perugia 3 dicembre 1952, in *Giust. Civ.*, 1953, p. 666 et MARMOCCHI, *Scrittura privata*, in *Riv. Not.*, 1987.

¹⁵ Cfr. paragrafo precedente, p. 28-29.

l'applicazione della stessa chiave privata a documenti informatici che divergono anche “per una sola virgola”, dà come risultato due firme digitali diverse; e che l'associazione di una firma digitale ad un documento diverso da quello su cui è stata creata, comporterebbe l'esito negativo della procedura di verifica a mezzo della chiave pubblica corrispondente.

Le differenze e le analogie fin qui rilevate non sono di ostacolo, comunque, all'affermazione della piena equipollenza tra sottoscrizione tradizionale e firma digitale (come risulta, peraltro, dall'art. 10 comma 2 del D.P.R. 513/97: *“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”*), sol che si consideri che in tanto ha senso parlare di requisiti della sottoscrizione, fintantoché questi si rivelino necessari a garantire le tre funzioni (funzione indicativa, dichiarativa, probatoria) cui la sottoscrizione è teleologicamente preordinata.

Ci troviamo, in altre parole, di fronte a un rapporto da “mezzo” (i requisiti di cui sopra) a “fine” (la c.d. funzione di imputabilità), che fermo restando il “fine” (la c.d. funzione di imputabilità), indipendentemente dal tipo di supporto, cartaceo o informatico, su cui si opera, legittima il mutamento dei requisiti in relazione al tipo di firma in concreto utilizzata.

Appare, dunque, corretto definire la firma digitale come “*strumento impersonale di attribuzione dell'identità personale dell'autore del documento*”¹⁶³.

¹⁶³ Occorrerà, naturalmente, anche la certificazione della chiave corrispondente perché il destinatario del documento sottoscritto possa raggiungere la certezza sull'identità del mittente. Dal punto di vista di quest'ultimo, tuttavia, la firma digitale vale a consacrare il suo rapporto di paternità con il testo sottoscritto, espressa proprio mediante la volontà dell'apposizione della firma stessa. Così ROGNETTA, *La firma digitale e il documento informatico*, cit.

CAPITOLO II

LA FIRMA DIGITALE IN ITALIA

1. QUADRO DI RIFERIMENTO NORMATIVO

Con l'emanazione della L. 59/97 e l'entrata in vigore dei regolamenti di delegificazione (art. 17 comma 2, l. 400/88) "attuativi" della delega contenuta nell'art. 15 della stessa (precisamente, il D.P.R. 513/97 e il successivo D.P.C.M. 8 febbraio 1999, attuativo dell'art.3 comma 1 del D.P.R. ¹¹) l'Italia è stato uno dei primi paesi a livello comunitario a darsi una regolamentazione organica relativa alla firma digitale.

Infatti, al tempo dell'emanazione delle succitate norme, tra i paesi membri dell'Unione Europea poteva operarsi una distinzione fra Stati che avevano regolamentato la materia del documento informatico e della firma digitale e più in generale il settore delle telecomunicazioni, e Stati che stavano avviando dibattiti e predisponendo proposte di legge.

¹¹ L'art 3 del D.P.R. 513/97 rubricato "Requisiti del documento informatico" al primo comma, così dispone: "Con decreto del Presidente del Consiglio dei Ministri, da emanare entro 180 giorni dall'entrata in vigore del presente regolamento, sentita l'Autorità per l'Informatica nella Pubblica Amministrazione sono fissate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici."

Così, in Germania è stata approvata la legge 22 luglio 1997 sulle firme digitali (BGB1. I. p. 1872), *Gesetz zur digitalen Signatur (Signaturgesetz – SigG)*; in Francia è stata adottata una legge sulle telecomunicazioni (*Loi n. 96-659 du 26 juillet 1996 de règlementation des télécommunication*), che garantisce un accesso semplice e conveniente a tutte le infrastrutture e ai servizi di telecomunicazione, nonché un decreto del Primo ministro (*Dècret n. 92-1358 du 28 décembre 1992*) che definisce le dichiarazioni sulle forniture di esportazione e di utilizzazione di mezzi e di prestazioni crittografiche, limitatamente quindi ad uno specifico settore.

Nel Regno Unito, precisamente nel marzo 1997, fu avviata una pubblica consultazione sulla regolamentazione dei terzi garanti o autorità di certificazione (*Licensing of trusted third parties for the provision of encryption services – public consultation paper on detailed proposals for legislation*).

Paesi Bassi, Danimarca, Belgio e Svezia erano anch'essi fermi ad uno stadio, diciamo così, embrionale di approccio alla materia.

Conseguentemente, nel panorama europeo, solamente Italia e Germania si erano dotate di un'organica disciplina della materia *de qua*.

Tornando alle scelte del legislatore nostrano, appare quanto mai dubbia, sotto un profilo e sistematico e costituzionale, la decisione di rimettere alla potestà regolamentare del Governo la disciplina della materia in oggetto (art 15 L.59/97).

Per quanto riguarda il primo aspetto, infatti, l'inserimento di una norma di tale portata all'interno di una legge avente ad oggetto il decentramento e la semplificazione amministrativa appare quantomeno criticabile sotto il profilo dell'opportunità, se si considera che l'art. 15 comma 2 concerne anche i rapporti fra privati.

Inoltre, sempre sotto il profilo dell'opportunità, ha suscitato critiche la scelta del legislatore di sottrarre al dibattito parlamentare, affidando tale compito al Governo, tramite lo strumento dei regolamenti di delegificazione ex art. 17 comma 2 della L. 400/88, la valutazione sul *come* andare ad "incidere", con la nuova normativa, sulla disciplina di concetti giuridici-base (come *validità, rilevanza, efficacia, prova documentale, scrittura privata* ecc.), e sollevando al contempo, data l'esiguità della delega (l'art. 15 cit., infatti, si limita a statuire la rilevanza e validità degli atti e documenti formati con strumenti informatici o telematici, rinviando per tutto il resto a regolamenti successivi), dubbi di costituzionalità di quest'ultima per violazione dell'art. 76 Cost.¹²⁵.

A mente il disposto dell'art. 17 comma 2, L. 400/88, il quale stabilisce che "con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei Ministri, sentito il Consiglio di Stato, sono emanati i regolamenti per la disciplina delle materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi della Repubblica,

¹²⁵ L'art. 76 Cost., che va coordinato con l'art. 70 Cost., espressione del principio costituzionale della separazione dei poteri, così recita: "L'esercizio della funzione legislativa non può essere delegato al Governo se non con determinazione dei principi e criteri direttivi e soltanto per tempo limitato e per oggetti definiti".

autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari" non si può non convenire con chi reputa costituzionalmente illegittimo l'art. 15 cit. perché risolvendosi, di fatto, in una delega in bianco al Governo, di guisa che non possa ritenersi il D.P.R. 513/97 attuativo-integrativo dei principi stabiliti dalla legge autorizzatrice, che "per essere così generali, tutto o quasi potrebbe risultarne attuazione-integrazione"³.

Come sosteneva, infatti, Paladin⁴ "occorre pur sempre che le norme legislative attribuenti poteri siffatti indichino con precisione la legislazione derogabile o modificabile all'atto di entrata in vigore dei regolamenti. Diversamente, infatti, non sarebbe più il legislativo ma l'esecutivo stesso a stabilire in che misura e con quali effetti la normazione regolamentare sia destinata ad alterare la disciplina di legge: nel qual caso, però, risulterebbero illegittimi non solo i regolamenti ma – prima ancora – le leggi che avessero reso possibili conseguenze così contrastanti con l'ordinamento costituzionale delle fonti del diritto"⁵.

³ Così L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, Giust. Civ., II, 1998, p.267-68. Nello stesso senso anche la dottrina dominante.

⁴ PALADIN, *Diritto Costituzionale*, II ed., Padova, 1996, p.227 ss.; ID., *Le fonti del diritto italiano*, Bologna, 1992.

⁵ Nello stesso senso G.U. RESCIGNO, *Corso di diritto pubblico*, IV ed., Bologna, 1994. In base a quanto riportato, non pare condivisibile la tesi avanzata da PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, in Riv. Not., 1997, p.575 ss., secondo il quale il D.P.R. 513 dovrebbe sussumersi nella categoria dei regolamenti di attuazione e non di quelli di delegificazione, di guisa che un eventuale contrasto tra norma codicistica (legge ordinaria) e

Passando ora all'esame della normativa che qui brevemente si commenta, e riservandomi una più approfondita trattazione degli argomenti a mio giudizio più interessanti nei paragrafi che seguono, può subito notarsi come il legislatore delegato non abbia inteso innovare in tema di principi, ma abbia preferito, di regola, la strada dell'adeguamento delle norme già esistenti di diritto comune a quella che è la nuova realtà rappresentata dalla firma digitale e dal documento informatico (cfr. ad esempio l'art. 5 del D.P.R. 513 in relazione agli artt. 2702 e 2712 c.c.).

Quanto detto è ribadito dalla stessa relazione di accompagnamento al D.P.R. 513/97, là dove si puntualizza che "il criterio adottato, per la formulazione delle norme autorizzate, consiste nel tentativo di adattare le norme vigenti (in particolare la disciplina in materia di efficacia probatoria degli atti e dei documenti del codice civile) alle nuove realtà informatiche e telematiche, estendendo la portata delle regole tecniche, individuate dall'Autorità per l'Informatica nella Pubblica Amministrazione per la formazione, la trasmissione e la conservazione del documento informatico, anche ai privati".

Strutturalmente, il D.P.R. 513 si presenta composto da ventidue articoli a loro volta suddivisi in tre capi, attinenti rispettivamente alla enunciazione di principi generali (artt. 1-9), alla disciplina della firma digitale (artt. 10-19) e infine alla predisposizione di norme di attuazione riguardanti lo sviluppo dei

norma regolamentare produrrebbe l'abrogazione della prima in forza, non del regolamento ma, della legge da cui quest'ultimo promana. A tale interpretazione osta però l'esplicito richiamo che l'art. 15 L. 59/97 fa all'art. 17 comma 2 della L.400/88 (regolamenti di delegificazione).

sistemi informativi automatizzati della P.A. e la gestione dei flussi documentali interamministrativi.

In realtà, tale suddivisione non va intesa in modo rigido, dato che alcune norme sulla firma digitale sono contenute nel capo I, come, a titolo esemplificativo, quelle relative alla certificazione della coppia di chiavi (art. 8), all'efficacia probatoria del documento sottoscritto con firma digitale (art.5), al deposito della chiave privata (art.7). Inoltre, alcune disposizioni del capo II avrebbero trovato una migliore allocazione nel capo I, quali l'art. 13 relativo alla segretezza della corrispondenza telematica, l'art. 15 sui libri e scritture, l'art. 14 sui pagamenti informatici.

Seguendo un'impostazione propria dei paesi di *common law*, il D.P.R. in esame, si apre con una serie di definizioni giuridico-tecniche, la cui comprensione è indispensabile per un corretto "approccio" al sistema.

Fra tutte, e tralasciando quelle già citate in precedenza, spicca quella di documento informatico definito dall'art. 1 lett. a) del D.P.R. cit. come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Viene, quindi, adattata a quella che è la nuova realtà informatica la celebre definizione Carneluttiana di documento, e ne viene, al contempo, ampliato il contenuto poiché, stante l'equipollenza tra forma scritta e documento informatico sancita dall'art. 4 comma 1, ne deriva che qualsiasi informazione digitalizzabile, quindi anche suoni o filmati, possono acquistare la dignità probatoria della scrittura privata (art. 2702 c.c.), se il documento informatico è dotato di firma digitale (art. 5 comma 1), mentre, in difetto di quest'ultima,

il documento informatico in regola con i requisiti stabiliti dal D.P.R. 513 rimane comunque valido e rilevante a tutti gli effetti di legge (art. 2), ma acquista la dignità probatoria delle riproduzioni meccaniche ex art. 2712 cc., facendo piena prova dei fatti, atti o dati in esso rappresentati se colui contro il quale è prodotto non ne disconosce la conformità ai fatti, atti o dati medesimi (art. 5 comma 2): risultati, questi ultimi, raggiungibili grazie alla completa equiparazione tra sottoscrizione tradizionale e firma digitale, sancita dall'art. 10 comma 2: *“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”*.

Il richiamo che l'art. 4 fa alla soddisfazione del requisito della forma scritta, quando siasi in presenza di un documento informatico conforme alle disposizioni del D.P.R. 513/97, deve intendersi come riferibile alla forma scritta *ad substantiam* (art. 1350 c.c.), prescritta dalla legge a pena di nullità, ed implica che il documento elettronico, a differenza di quello cartaceo, soddisfa il requisito legale della forma a prescindere dalla apposizione della firma autografa, anche se invero deve rispettare le norme tecniche stante il richiamo operato dall'art. 3 al d.p.c.m. 8 febbraio 1999 (norme che dovranno aggiornarsi con cadenza almeno biennale^{36a}).

^{36a} La cadenza biennale, di cui al comma 2 dell'art. 3 del D.P.R. 513, va intesa nel senso che almeno ogni due anni dovrà esservi un riesame dello stato della tecnica, al termine del quale si deciderà se adeguare o meno le ultime prescrizioni. In caso affermativo sarà opportuno che il provvedimento di aggiornamento in questione conceda una ragionevole *vacatio legis*, dal momento che dovranno essere adeguati i relativi *software* per potersi avvalere delle nuove specifiche tecniche. In presenza di nuove disposizioni, infatti, è da ritenere che le precedenti specifiche tecniche non possano più essere ritenute conformi alla l. n. 59 del 1997: quando un

Dovranno peraltro essere precisate dal legislatore, mancando ogni disciplina in merito e nel D.P.R. 513 e nel D.P.C.M. 8 febbraio 1999, le procedure specifiche per la trascrizione dei documenti informatici con firma digitale autenticata, come tali equiparati, ai sensi del combinato disposto degli artt. 5 comma 1 e 16⁷⁷, alle scritture con sottoscrizione autenticata, ai fini di cui agli artt. 2643 e 2657 c.c.

L'art. 8 del D.P.R. 513, al primo comma, prescrive che per la formazione di un documento informatico valido e rilevante a tutti gli effetti di legge è necessario utilizzare un sistema di crittografico asimmetrico, rispondente alle specifiche tecniche di cui agli artt. 2 e 3 del d.p.c.m. cit., munendosi di una idonea coppia di chiavi⁷⁸ e rendendo pubblica una di esse mediante la procedura di certificazione.

D.P.R. stabilisce nuovi accorgimenti tecnici, dovrà intendersi che solo questi avranno la rilevanza giuridica stabilita dalla l. n. 59 del 1997 e dal D.P.R. 513 del 1997. Le specifiche tecniche precedenti avranno un qualche rilievo giuridico, ma non certo l'efficacia massima permessa dal D.P.R. 513; non sarà però vero il contrario, nel senso che un eventuale sistema di sicurezza nuovo e non ancora "vagliato" dall'emanando provvedimento potrà avere la rilevanza sostanziale e probatoria massima prevista dal D.P.R. 513 se, in base ad apposita consulenza tecnica di causa si dimostrasse non meno sicuro dei sistemi contemplati dal decreto sulle specifiche tecniche vigente.

⁷⁷ L'art. 16 del D.P.R. 513 al primo e secondo comma, dispone che: "Si ha per riconosciuta, ai sensi dell'art. 2703 c.c., la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato. 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'art. 28, primo comma, della legge 16 febbraio 1913, n.89". Per i problemi ermeneutici sollevati da tale norma si rinvia al par. 9 di questo capitolo.

⁷⁸ L'idoneità della coppia di chiavi è data dalla loro lunghezza che il d.p.c.m. 8 febbraio 1999 fissa, all'art. 4 comma 6 dell'allegato tecnico, nella misura minima di 1024 bit. La robustezza delle chiavi, a mente i principi, richiamati al par. 3 del cap. I, di complementarità e indipendenza delle chiavi, è data dal fatto che, in base al concetto di "complessità computazionale", risulti di fatto impossibile risalire alla chiave privata dalla chiave pubblica ovvero il risultato ottenibile tramite

Quest'ultima è definita dall'art.1 lett. h) del D.P.R. cit. come 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.

L'attività di certificazione è svolta da nuovi soggetti di diritto detti *Certificatori* inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività (regime autorizzatorio: cfr. artt. 16, 17 e 18 del d.p.c.m. 8 febbraio 1999), in un apposito elenco (il cui contenuto è specificato dall'art. 15 dell'allegato tecnico al d.p.c.m.), consultabile *on-line*, predisposto tenuto e aggiornato a cura dell'A.I.P.A. e dotati di specifici requisiti relativi sia alla forma societaria adottabile (s.p.a., con capitale sociale non inferiore a 12,5 miliardi) sia al profilo organizzativo-gestionale delle imprese in questione (questi requisiti trovano ulteriore specificazione agli artt. 45- 51 del d.p.c.m.).

La sussistenza, in capo ai certificatori, dei requisiti richiesti per poter svolgere l'attività di certificazione è costantemente monitorata dall'A.I.P.A. e il venir meno degli stessi è causa di cancellazione dall'elenco (art.18 d.p.c.m.).

questa operazione (calcolo della chiave privata ai fini di falsificazione di un documento informatico) sia trascurabile rispetto al tempo necessario per ottenerlo.

La procedura di certificazione può essere svolta, altresì, da certificatori appartenenti ad altri Stati membri dell'Unione europea o dello Spazio economico europeo, se dotati di requisiti equivalenti a quelli sopra richiamati, e da certificatori appartenenti a Stati non appartenenti all'Unione Europea con i quali l'Italia abbia stipulato accordi di riconoscimento reciproco relativamente alle specifiche tecniche cui attenersi (art. 3 comma 3 del d.p.c.m.).

L'art. 21 del d.p.c.m. prevede la c.d. *cross certification*, cioè la possibilità che ha ciascun certificatore di riconoscere nel proprio ambito la validità di certificazioni effettuate da altre s.p.a. partecipanti al sistema, come delineato dall'art. 8 comma 3 del D.P.R. 513⁹⁹.

I certificatori potranno intervenire nel mercato vendendo il *software* di produzione delle chiavi asimmetriche di criptazione, oppure lasciando al cliente la libertà di procurarsene altrove tra quelli offerti sul mercato e compatibili con i sistemi di controllo del certificatore stesso.

Il rilascio del certificato deve essere, preventivamente, subordinato alla richiesta di registrazione presso il certificatore, la quale deve essere redatta per iscritto dall'interessato e conservata a cura del certificatore per almeno dieci anni. La registrazione è preceduta dalla verifica dell'identità fisica del richiedente (*rectius*: del titolare delle chiavi) operata dal certificatore in base a modalità dallo stesso definite. A seguito della registrazione dell'interessato, il

⁹⁹ In particolare, con l'accordo di certificazione, un certificatore emette a favore dell'altro un certificato relativo a ciascuna chiave di certificazione che viene riconosciuta nel proprio ambito.

certificatore gli attribuirà un codice identificativo di cui garantisce l'univocità nell'ambito dei propri utenti: i codici possono essere più di uno a seconda dei ruoli per i quali il soggetto registrato può firmare (art. 22 d.p.c.m.).

È importante sottolineare come, ex art. 24 d.p.c.m., sia posto a carico del certificatore un obbligo di informazione, verso il richiedente la registrazione, circa gli obblighi da quest'ultimo assunti relativamente alla protezione della segretezza della chiave privata. Obbligo che costituisce "specificazione" di quanto stabilito all'art. 9 comma 1 del D.P.R. 513, che pone a carico dell'utilizzatore di un sistema di firma digitale (e avendo utilizzato il legislatore il termine *chiunque* ne consegue *de plano* l'applicabilità della prescrizione sia nei confronti del certificatore che del titolare della coppia di chiavi) una responsabilità oggettiva per danni causati a terzi, quando non riesca a dimostrare di avere adottato tutte le misure organizzative e tecniche idonee ad evitare il danno medesimo. È evidente il richiamo all'art. 2050 c.c., avendo il legislatore inquadrato l'utilizzazione di un sistema di firma digitale come attività pericolosa, vale a dire attività caratterizzata da un'intrinseca potenzialità lesiva superiore alla media¹⁰.

¹⁰ In sede di esegesi dell'art. 2050 c.c., l'opinione tradizionale individua nella fattispecie in esame un'ipotesi di responsabilità fondata sulla colpa, quindi un'applicazione dell'illecito aquiliano ex art. 2043 c.c., caratterizzata unicamente da un'inversione dell'onere della prova, per quanto riguarda l'elemento della colpa, configurando quindi una presunzione *iuris tantum* che grava sulla parte che si suppone autrice del danno. Degna di massimo rilievo appare tuttavia la tesi secondo cui l'art. 2050 c.c. non si limita ad un'inversione dell'onere della prova ma detta una regola di responsabilità più rigorosa di quella prevista in termini generali, essendo stata prevista la responsabilità di chi esercita l'attività pericolosa per non avere adottato "tutte le misure idonee a evitare il danno". Ne deriva che in relazione all'art. 9 comma 1 del D.P.R. 513/97, la responsabilità per danno dell'utilizzatore di un sistema di firma digitale sarà valutata con un giudizio *ex post*, configurando nella mancanza di adeguate misure tecniche e organizzative, un

Segue quindi la richiesta di certificazione della coppia di chiavi (*rectius*: della chiave pubblica) nella quale il soggetto interessato specificherà quali tra le informazioni suppletive, relative a una coppia di chiavi di sottoscrizione (cfr. art. 11 comma 3, d.p.c.m.), non vuole siano inserite nel certificato¹¹⁹: la richiesta deve essere conservata a cura del certificatore per un periodo almeno decennale (art. 27 d.p.c.m.).

Prima di emettere il certificato il certificatore è tenuto, previamente, ad effettuare un triplice controllo consistente nella verifica dell'autenticità della richiesta, nella verifica della insussistenza di una precedente certificazione della chiave pubblica in questione da parte di altro certificatore iscritto nell'elenco tenuto dall'A.I.P.A. (al fine di evitare il pericolo che la chiave pubblica di cui si chiede la certificazione corrisponda a chiave privata il cui titolare sia soggetto diverso dal richiedente), nel richiedere la prova del possesso della chiave privata e verificare il corretto funzionamento della coppia di chiavi.

Se queste verifiche hanno esito positivo, il certificato viene pubblicato *on-line* mediante l'inserimento nel registro dei certificati, i c.d. *key – repositories*, altrimenti la richiesta verrà rigettata (art 28 d.p.c.m.).

Il registro dei certificati deve essere raggiungibile dal destinatario di un documento firmato digitalmente indipendentemente dalla conoscenza che

caso di responsabilità oggettiva. In questo senso ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica"*, in Riv. Dir. Inf., 1997.

questi abbia dell'indirizzo elettronico corrispondente: è pertanto stabilito che attraverso la firma digitale sia possibile rilevare gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione (art. 10 comma 7).

Dall'analisi delle summenzionate norme emerge come il certificato (*rectius*: l'attività di certificazione) supplisca alla assenza di relazione fisica tra firma digitale e sottoscrittore con una relazione "digitale", che documenta la corrispondenza, anche nel tempo, tra la chiave pubblica e il suo titolare rigorosamente identificato e, conseguentemente, la corrispondenza delle firme digitali da lui apposte (ne deriva, quindi, l'impossibilità da parte di quest'ultimo di negare, dopo la verifica - positiva - della firma digitale con la corrispondente chiave pubblica, che il documento informatico prodotto contro di lui in giudizio sia stato firmato con la chiave privata di cui lui risulta essere titolare: c.d. principio del *non - repudiation*¹¹²).

Riassumendo: la certificazione della chiave pubblica è contenuta in un documento informatico definito come certificato, a sua volta firmato digitalmente dalla parte emittente. Il certificato, una volta emesso, è valido per (*rectius*: conferisce validità a) una serie indeterminata di firme digitali

¹¹¹ Per il contenuto minimo-necessario di ogni certificato e per la distinzione fra chiavi di sottoscrizione, chiavi di certificazione e chiavi di validazione temporale, in relazione ai soggetti abilitati alla loro generazione, vedasi quanto riportato al par. 4, cap. I, nota 7.

¹¹² Conformemente, l'art. 10 comma 3 e 4 del D.P.R. 513 dispongono che: "3. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. 4. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata".

successive, a meno che non intervengano determinate cause invalidanti (scadenza, revoca sospensione).

Abbiamo più sopra visto che la durata del certificato è stata stabilita dall'art.1 lett. h) del D.P.R. 513 nella misura massima di tre anni.

Ebbene, vi sono ipotesi, disciplinate rispettivamente agli artt. 30-32 e artt.34-36 del d.p.c.m., in cui può aversi la cessazione anticipata della validità di un certificato (revoca con effetti *ex nunc*: art. 10 comma 5 D.P.R. 513), oppure la sua sospensione in via cautelare: eventi che producono l'effetto di una mancata sottoscrizione nel caso di utilizzo di una chiave privata revocata, sospesa o scaduta.

La revoca e la sospensione dei certificati possono essere disposte dal certificatore in ipotesi tassativamente determinate:

- a) apposita richiesta del titolare o del terzo dal quale derivino i poteri di quest'ultimo;
- b) perdita del possesso della chiave o provvedimento dell'autorità ovvero acquisizione della conoscenza di cause limitative della capacità del titolare;
- c) sospetti di abusi o falsificazioni (art. 9 lett. h))

In particolare, il certificatore deve revocare il certificato quando si verifica un evento che incide sulla titolarità della chiave, in modo che tal evento sia subito conoscibile dai terzi, e con efficacia non retroattiva, onde garantire la massima tutela dell'*affidamento*.

Dalla lettura combinata dell'art. 9 comma 2, lett. h) del D.P.R. 513/97 e dell'art. 29 dell'allegato tecnico emerge che legittimati a inoltrare la richiesta di revoca del certificato sono: il titolare della chiave privata corrispondente, il certificatore medesimo, il terzo interessato¹³⁵. La revoca del certificato deve essere prontamente pubblicata *on-line* in un'apposita lista dei certificati revocati (CRL) curata dal certificatore: la garanzia circa il momento dal quale decorrono gli effetti della revoca è data dall'apposizione di una "marca temporale" (quest'ultima, altro non è che il prodotto di una procedura di "validazione temporale" cioè, secondo la definizione datane dall'art. 1 lett. i) del D.P.R. 513, "la procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi").

Se la richiesta di revoca proviene dal titolare, deve contenere la motivazione e l'indicazione della decorrenza. Il certificatore, ricevuta la richiesta, deve verificarne l'autenticità e procedere alla revoca entro il termine richiesto. Se ciò non è possibile procederà alla sospensione del certificato.

Se la revoca avviene su iniziativa del certificatore, questi, salvo i casi di motivata urgenza, deve darne comunicazione al titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale il certificato non è più valido.

¹³⁵ Terzo interessato può essere una società che chiedi la revoca del certificato relativo alla chiave pubblica corrispondente alla chiave privata di un amministratore delegato non più dotato di poteri rappresentativi. Come sappiamo, infatti, l'art. 11 dell'allegato tecnico individua come contenuto eventuale del certificato relativo a chiavi di sottoscrizione la menzione di eventuali poteri di rappresentanza. Questa previsione, costituisce specificazione dell'obbligo che l'art. 9 lett. c) del D.P.R. 513 impone a carico del certificatore di specificare, su richiesta dell'istante, e

Infine, se la richiesta di revoca proviene dal terzo interessato, questa deve assumere la forma scritta ed essere corredata della documentazione giustificativa. Il certificatore deve notificare la richiesta al titolare, il quale, altrimenti potrebbe ignorare l'esistenza della richiesta di revoca.

La stessa procedura, con gli adattamenti del caso, deve essere seguita in caso di richiesta di sospensione del certificato, la quale dovrà essere pubblicizzata *on-line* mediante l'inserimento nelle liste dei certificati sospesi (CSL), con la conseguente apposizione di una marca temporale, al certificato sospeso, al fine di rendere opponibile l'invalidità temporanea ai terzi.

La revoca e la sospensione hanno efficacia dal momento della pubblicazione, a meno che il soggetto cui è stato revocato o sospeso il certificato, dimostri che tutte le parti interessate ne erano a conoscenza anche prima della pubblicazione; si tratta di una pubblicità dichiarativa o *notificativa*, nel senso che l'avvenuta pubblicazione crea in capo ai terzi una presunzione *iuris et de iure* di conoscibilità (art. 10 comma 5 D.P.R. 513).

Così descritta, brevemente, la normativa di riferimento ai fini della presente trattazione, verranno ora approfondite, nei paragrafi che seguono, le tematiche della "novella" che hanno suscitato maggiori problemi interpretativi e tralasciate, invece, quelle che, a mio avviso, hanno

con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite.

un'importanza residuale rispetto a quello che in questa sede si viene argomentando.

2. IL DOCUMENTO INFORMATICO: REQUISITI, VALIDITÀ ED EFFICACIA PROBATORIA

La validità e la rilevanza del documento informatico sono state sancite dall'art. 15 della legge n. 59 del 1997.

Il contenuto di questa norma, come sappiamo, è stato poi puntualizzato dal D.P.R. 513 del 1997, che, in particolare, dopo la definizione di “documento informatico” data dall'art. 1 lett. a), ne sancisce all'art. 2 la validità e rilevanza a tutti gli effetti di legge qualora risulti conforme alle prescrizioni del regolamento medesimo. Il successivo art. 4 stabilisce poi la piena equiparabilità tra la forma scritta e la forma elettronica.

Appaiono opportune, preliminarmente, due considerazioni. La prima, di ordine semantico, riguarda l'evidente *lapsus* del legislatore delegato circa la successione logica dei termini “validità” e “rilevanza”. Come rileva, infatti, Tommasini non può esprimersi un giudizio di validità relativamente ad un atto o un fatto se questo non sia stato previamente ritenuto rilevante, e quindi degno di tutela, dall'ordinamento giuridico (arg. ex art. 1322 c.c.). Per cui “il giudizio in termini di validità – invalidità e la qualifica di rilevanza – irrilevanza hanno entrambi un nesso con l'efficacia, ma operano su piani diversi: il fatto è rilevante per ciò solo che l'interesse prospettato entra nell'ambito degli interessi presi in considerazione dal diritto; il fatto è valido se l'interesse prospettato è giudicato conforme agli interessi o ai valori del

sistema...”¹□: pertanto il primo giudizio, quello di rilevanza, risulta propedeutico, e quindi condizionante, il secondo, quello di validità.

La seconda considerazione, di ordine “classificatorio”, riguarda la configurabilità o meno della forma elettronica come *tertium genus* rispetto alle due tradizionali forme di estrinsecazione della volontà negoziale (forma scritta e forma orale).

A parere di chi scrive, è preferibile la tesi di chi sostiene che il termine “forme” utilizzato dal legislatore all’art. 15 della legge n. 59 del 1997, non abbia una valenza tecnica, e quindi classificatoria, ma solamente descrittiva, equivalente ad un sinonimo di “modalità” di documentazione del contenuto contrattuale. Se è vero infatti che la documentazione informatica del contenuto contrattuale è in grado di “invadere” nuovi spazi e di superare i confini tradizionalmente impostigli, dato che potrà aversi documentazione digitale della conclusione di un contratto attraverso la ripresa video dei contraenti che emettono le dichiarazioni costituenti l’accordo (e l’immagine, così digitalizzata, potrà essere firmata digitalmente soddisfacendo i requisiti imposti sia dall’art. 1350 c.c. che dall’art. 2702 c.c.)²□, è anche vero che la scritturazione avverrà pur sempre attraverso il linguaggio dei *bit*; ritengo,

¹□ Così TOMMASINI, *Invalidità*, in Enc. dir., XXII, Milano, 1971, pp. 580-581.

²□ In questo senso F. RIZZO, *Valore giuridico ed efficacia probatoria del documento informatico*, in Riv. dir. inf., 2000, p. 216 e nota n. 20, p. 218.

pertanto, preferibile, come sostenuto da Petrelli³³, collocare il documento informatico in un rapporto di genere a specie rispetto alla forma scritta.

Il riconoscimento a tutti gli effetti di legge della forma elettronica, sancita dall'art. 4 cit., consente ora di porre in essere quelle fattispecie contrattuali e negoziali per le quali l'art. 1350 cc. pone come requisito minimo di validità la forma scritta³⁴: ne deriva l'espreso riconoscimento della scrittura privata elettronica e la sua equiparabilità alla scrittura privata tradizionale, pur in difetto della sottoscrizione autografa dell'autore dello scritto.

Quanto detto trova conferma nell'art. 5 del D.P.R. 513, rubricato "Efficacia probatoria del documento informatico", che stabilisce per il documento informatico munito di firma digitale la stessa efficacia attribuita alla scrittura privata dall'art. 2702, mentre il documento informatico munito dei requisiti previsti dal regolamento stesso ha l'efficacia probatoria che il codice attribuisce alle riproduzioni meccaniche ex art 2712 c.c. e soddisfa l'obbligo previsto dagli artt. 2214 ss. cc. e da ogni altra analoga disposizione legislativa o regolamentare.

Una lettura poco attenta dell'articolo sopra riportato potrebbe portare a chiedersi quando un documento informatico acquisti l'una o l'altra efficacia, dato che per la validità e rilevanza dello stesso in entrambi i casi è richiesta la conformità al D.P.R. 513 (art. 2). Unica conclusione possibile, anche in virtù

³³ Cfr. G. PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, in Riv. not., 1997, p. 576.

³⁴ Come si vedrà in seguito al par. 10 non pare si possa configurare, in assenza di una specifica disposizione in tal senso, la possibilità di formare un atto pubblico notarile in forma digitale.

dell'esplicito richiamo che il primo comma fa all'art. 10, il quale riconosce la piena equivalenza tra firma digitale e sottoscrizione su supporto cartaceo, è interpretare il comma secondo nel senso che la conformità dovrà riguardare solo il regolamento, prescindendosi dall'apposizione di una valida firma digitale. Se ne deduce che l'efficacia probatoria dell'art. 2712 c.c. è propria del documento informatico anche se non sottoscritto digitalmente; d'altra parte non avrebbe alcun senso attribuire l'efficacia probatoria delle riproduzioni meccaniche solo al documento firmato digitalmente quando il primo comma dell'art. 5 gli attribuisce l'efficacia probatoria, ben più penetrante, della scrittura privata autenticata, riconosciuta o verificata giudizialmente.

Rimane poi da chiedersi quali siano i requisiti del regolamento in oggetto, diversi dalla firma digitale, che un documento informatico deve soddisfare per ottenere la particolare efficacia probatoria propria delle riproduzioni meccaniche. La soluzione non è affatto agevole, anche perché il D.P.R. in oggetto è quasi interamente dedicato alla firma digitale e lo stesso dicasi per il D.P.C.M. dell'8 febbraio 1999 che riguarda principalmente requisiti e modalità di utilizzo del sistema crittografico a chiavi asimmetriche e l'attività di certificazione. Non è quindi dato riscontrare alcuna norma che disciplini positivamente tali requisiti. Convenendo con quanto scrive Albertini⁵⁵, si potrebbero considerare soddisfatti i requisiti di cui sopra in presenza di una mera conformità a quanto prescrive genericamente il D.P.R.: a) esistenza di

un documento informatico; b) trasmissione ad un indirizzo elettronico (solo in caso di sua spedizione); c) apposizione di una firma digitale con un *software* non rispettoso delle specifiche tecniche stabilite dall'allegato tecnico o non adottante un sistema di certificazione c.d. "verticale" (mi riferisco in particolare al P.G.P.), oppure apposizione di una firma digitale il cui certificato sia scaduto, revocato o sospeso.

Ne consegue che un qualsiasi accesso ad un sito *internet* o la ricezione di una *e-mail* formano "piena prova dei fatti rappresentati", a meno che il mittente contro cui venga prodotto in giudizio il documento informatico non ne disconosca la conformità ai fatti medesimi o neghi l'invio del documento all'indirizzo elettronico del destinatario.

A questo punto si tratta di stabilire se il richiamo che l'art. 5 primo comma fa all'art. 2702 c.c. riguardi solo il particolare tipo di efficacia di cui la scrittura privata autenticata, riconosciuta o verificata è dotata (prova legale vincibile solo con querela di falso), ovvero richiami l'intera fattispecie astratta e, per altro verso, a mente il secondo comma dell'art. 5, se il documento informatico - eventualmente contenente una dichiarazione negoziale - sottoposto alla disciplina di cui all'art. 2712 c.c., sia soggetto ad un onere di disconoscimento con preclusioni analoghe a quelle previste dagli artt. 214 ss. c.p.c. e, ancora, se il riferimento alla "piena prova" di cui all'art. 2712 c.c. implichi o meno la possibilità da parte del giudice di apprezzare liberamente le risultanze documentali non disconosciute.

⁵³ L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, in Giust. Civ., II, 1998, pp. 277-278.

Affronteremo prima il secondo ordine di problemi, perché pare potersi giungere, relativamente ad essi, ad una soluzione meno controversa sul piano dottrinale di quanto, invece, consenta l'ermeneutica delle norme che ha sollevato i primi.

Circa l'estensibilità analogica delle preclusioni cui fa riferimento il n.2 dell'art. 215 c.p.c. (“il disconoscimento della scrittura privata deve avvenire entro la prima udienza o la prima risposta successiva alla produzione”) alla fattispecie delineata dall'art. 2712 c.c. – quest'ultimo applicabile, per espresso disposto dell'art. 5 secondo comma D.P.R. 513, al documento informatico dichiarativo⁷⁶ non firmato digitalmente, ritengo sia preferibile dare risposta negativa.

A sostegno di tale tesi sembra orientata la dottrina largamente maggioritaria⁷⁷ sulla base della considerazione che, mentre il disconoscimento della scrittura privata ha ad oggetto la paternità del documento (il c.d. “contenuto estrinseco”), quello relativo alle “riproduzioni informatiche” ha ad oggetto la conformità dei fatti in esso rappresentati alla realtà. La contestazione ha pertanto ad oggetto il contenuto del documento (il

⁷⁶ Può operarsi, infatti, una distinzione fra documenti *dichiarativi*, incorporanti una dichiarazione del soggetto che ha formato il documento stesso, e documenti *narrativi*, incorporanti informazioni che non siano riconducibili ad una manifestazione di volontà del loro autore. In particolare, per documento dichiarativo, può intendersi soltanto il documento che, oltre a rappresentare la dichiarazione, rappresenta anche il soggetto da cui proviene. In altre parole il documento che contiene anche la prova della sua provenienza soggettiva, la quale coincide con la prova della sua formazione. Cfr. CARNELUTTI, *La prova civile, parte generale*, Milano, 1915, e, per quanto riguarda la materia in oggetto GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, in Riv. trim. dir. proc. civ., 1998.

⁷⁷ Vedi per tutti RICCI, *Aspetti processuali della documentazione informatica*, Riv. trim. dir. e proc. civ., 1994, pag. 872.

c.d. “contenuto intrinseco”) e non la provenienza soggettiva del medesimo. Ration per cui non appare giustificabile l'estensione delle preclusioni di cui sopra alla fattispecie in esame.

Per quanto riguarda, invece, il riferimento che l'art. 2712 c.c. (letto nell'ottica dell'art. 5 comma 2 D.P.R. 513) fa all'efficacia di “piena prova” circa i fatti, rappresentati in un documento informatico non firmato ovvero firmato secondo modalità diverse da quelle stabilite dal D.P.R. 513 (ad es. il PGP), appare preferibile optare per la tesi che non configura questo riferimento fatto dal legislatore come attributivo dell'efficacia di prova legale.

Com'è noto, il giudice valuta la prova liberamente secondo il suo convincimento e apprezzamento (art. 116 c.p.c.), eccettuati i casi nei quali la legge stessa attribuisce l'efficacia di prova (da intendersi nel significato proprio del termine⁸⁰), legando le mani a chi giudica; quando trattasi di prova legale la legge ritiene una certa prova idonea *in modo preciso* a dimostrare un fatto, pertanto al giudice è inibita qualsiasi valutazione sul contenuto della stessa, dovendosi semplicemente attenere alle risultanze di quest'ultima, così come legalmente stabilito.

Considerato che quando il legislatore ha voluto definire una prova come legale lo ha fatto espressamente (come negli art.2702 e 2700: “...piena prova, fino a querela di falso...”), perché convinto del carattere di incontrovertibilità

⁸⁰ Come infatti sottolineato da CARNELUTTI, *Diritto e processo*, Roma, 1958, p. 153, la terminologia impiegata sia dalla legge che dai giudici nonché dalla dottrina è confusa e incerta perché, mentre la prova è in sé stessa un giudizio, di solito lo stesso termine viene utilizzato non per indicare un giudizio, ma per indicare i mezzi per il giudizio o addirittura il risultato positivo di questo.

dei fatti costituenti la medesima, appare, allora, preferibile interpretare la locuzione “piena prova” di cui all’art. 2712 c.c. come idoneità della prova a dimostrare l’accertamento di un fatto, ma non ad escludere automaticamente il libero apprezzamento del giudice o l’ammissibilità di prove contrarie.

Nel caso, quindi, di un documento informatico dichiarativo, non disconosciuto, firmato tramite l’utilizzo di un sistema di validazione “fuorilegge” (leggi: PGP e il relativo sistema di certificazione orizzontale) non si potrà, in alcun modo, attribuirgli l’efficacia di prova legale circa la provenienza soggettiva dello scritto e presuntivamente delle dichiarazioni in esso contenute.

Questo perché la prova legale della provenienza soggettiva di uno scritto digitale, può essere fornita solo nelle forme tipiche stabilite dal regolamento così come la prova legale della provenienza soggettiva di uno scritto tradizionale può essere data solo nelle ipotesi tipiche disciplinate dall’art. 2702⁹⁹.

Più sopra abbiamo visto che un documento informatico munito di firma digitale valida abbia efficacia di scrittura privata ai sensi dell’art. 2702 c.c.. Il rinvio fatto dall’art. 5 del D.P.R. n. 513 all’efficacia probatoria della scrittura privata ha diviso la dottrina, in seno alla quale sono individuabili due correnti interpretative. In particolare, può operarsi una distinzione tra autori che qualificano il richiamo di cui sopra come relativo alla sola efficacia

⁹⁹ Così GRAZIOSI, *Premesse...*, cit., p.525.

probatoria della sottoscrizione legalmente riconosciuta¹⁰, e autori che interpretano il richiamo dell'art. 5 come relativo all'intera fattispecie astratta dell'art. 2702 c.c. ritenendo, quindi, la firma digitale disconoscibile e verificabile giudizialmente¹¹.

Appoggiare l'una o l'altra tesi significa, rispettivamente, ritenere o meno la scrittura privata informatica, positivamente verificata con la chiave pubblica corrispondente, una prova legale *indipendentemente* dalla ricorrenza di quelle condizioni normative (artt. 2702-3 c.c. et art. 214 ss. c.p.c.) che la legge ritiene imprescindibili per l'acquisto di tale efficacia da parte della scrittura privata tradizionale. La questione, in altre parole, riguarda l'applicabilità o meno degli istituti del disconoscimento (artt. 214-15 c.p.c.) e della verifica (artt. 216-20 c.p.c.) alla scrittura privata informatica.

Nel paragrafo che segue si cercherà di dimostrare la bontà della prima delle due tesi (non – disconoscibilità della firma digitale), qui solo enunciata,

¹⁰ In questo senso ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente atti, documenti e contratti in forma elettronica*, in Riv. dir. e inf., 1997; ID., *La firma digitale quale fonte di certezze giuridiche*, intervento presso il convegno tenutosi a Camerino: "Documento informatico, firma digitale, commercio elettronico", 29-30 ottobre 1999, in www.unicam.it/ssdici/convegno_ott.html; GRAZIOSI, *Premesse per una teoria probatoria del documento informatico*, cit.; G. FINOCCHIARO, *Documento informatico e firma digitale*, in *Contratto e Impresa*, 1998; A. GENTILI, *Documento informatico e tutela dell'affidamento*, in riv. dir. civ., II, 1998; M. ORLANDI, *L'imputazione dei testi informatici*, in Riv. Not. 1998; C. MASSIMO BIANCA, *I contratti digitali*, in *Studium iuris*, II, 1998; BIANCA, *Diritto civile*, III, *Il contratto*, Milano, 2000.

¹¹ L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, cit.; F. DELFINI, *Forma e trasmissione del documento informatico nel reg. ex art. 15.2 L. 59/97*, in Riv. I Contratti, n. 6, 1997; G. ROGNETTA, *La firma digitale e il documento informatico*, cit.; F. DE SANTIS, *La disciplina del documento informatico. Il commento*, in *Corriere Giur.*, 1998; seppur enunciando la sua opinione in maniera sintetica cfr. G. PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, cit.; F. ORLANDI, *Il regolamento sul documento elettronico: profili ed effetti*, in Riv. dir. Comm. e diritto generale obblig., 1998; V. FEDELI, *Documento informatico e firma digitale: valore giuridico ed efficacia probatoria alla luce del decreto del Presidente della Repubblica 10 novembre 1997, N. 513*, in Riv. dir. Comm. e diritto generale obblig., 1998; F. FERRARI, *La nuova disciplina del documento informatico*, in Riv. dir. proc., 1999.

perché ritenuta, a parere di chi scrive, più aderente, da un lato, al contenuto della disciplina del documento informatico e, dall'altro, alla logica di un sistema crittografico asimmetrico così come delineato dal nostro legislatore.

3. (SEGUE) – SCRITTURA PRIVATA INFORMATICA E PROVA LEGALE

La scrittura privata (tradizionale), in sé considerata, non è idonea a dare sufficienti garanzie circa la sua provenienza soggettiva.

A tal fine il legislatore ha prescritto all'art. 2702 c.c. che essa costituisce prova legale della provenienza, del documento e presuntivamente delle dichiarazioni in esso contenute, dal suo sottoscrittore se, e solo se, essa risulti essere autentica.

La dottrina¹, specificando che per autenticità di uno scritto deve intendersi la coincidenza tra la persona che ha veramente apposto la sottoscrizione con la persona indicata dalla sottoscrizione stessa come autore di un documento, non ha mancato di ribadire che tale carattere acquista la scrittura privata solo quando con essa operino determinate condizioni normative (o espedienti integrativi secondo la definizione di Mandrioli²) ritenute imprescindibili dal legislatore per attribuirle la particolare forza probatoria di cui all'art. 2702: "... piena prova, fino a querela di falso".

Questi espedienti integrativi sono ricavabili da una combinata lettura degli artt. 2702 e 2703 c.c.

Il primo di questi articoli statuisce che la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi la sottoscrittà, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. Il successivo

¹ P. SCHLESINGER, *La scrittura privata*, in Jus, 1961, p.447

² C. MANDRIOLI, *Corso di diritto processuale civile*, II, Torino, 1995, p. 190 ss.

art. 2703 c.c. prescrive che si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

È possibile, quindi, individuare, a mente gli articoli del codice di rito richiamati dalle summenzionate norme, le seguenti cinque condizioni normative che, operando insieme con la sottoscrizione, portano il legislatore ad equiparare l'efficacia probatoria della scrittura privata a quella dell'atto pubblico (art. 2699-2700 c.c.), limitatamente all'aspetto della sua provenienza:

- riconoscimento della sottoscrizione da parte di colui contro il quale la scrittura viene prodotta;
- autenticazione della sottoscrizione ex art. 2703;
- contumacia della parte contro cui la scrittura è stata prodotta (art. 215 n.1 c.p.c.);
- mancato disconoscimento tempestivo della parte contro cui la scrittura è stata prodotta;
- esito positivo dell'istanza di verifica, azionata dalla parte produttrice la scrittura privata tempestivamente disconosciuta.

Si tratta ora di stabilire se anche la scrittura privata informatica debba necessariamente sposare l'intera disciplina concepita per la scrittura privata tradizionale oppure rispetto ad essa possa parlarsi di disapplicazione, dovendosi considerare il sistema di firma digitale in grado di perseguire, *prima e fuori* della fase giudiziale, quanto viene raggiunto, in sede processuale, dall'istanza di verifica.

La dottrina che interpreta il richiamo contenuto nell'art. 5 comma 1 D.P.R. 513 come comprensivo dell'intera fattispecie normativa descritta dall'art. 2702 c.c. sostiene le sue conclusioni facendo leva, sostanzialmente, su un triplice ordine di argomentazioni.

La prima, si basa su un raffronto tra quanto disposto dall'art.5 del D.P.R. 513 e dall'art. 16 del medesimo regolamento ("*Firma digitale autenticata*"). Si sottolinea che là dove il legislatore ritiene opportuno modificare o adattare alla nuova realtà informatica quello che è l'impianto codicistico tradizionale lo dice espressamente⁽³⁾; ne deriva allora che "stante la presenza nel nostro ordinamento di due precisi elementi della fattispecie costitutiva del vincolo probatorio legale cioè l'autenticazione, da un lato, e il riconoscimento, espresso o tacito ex art. 215 c.p.c., dall'altro, deve ritenersi – in assenza di indici contrari – non certo che quest'ultimo sia stato escluso, bensì, piuttosto e al contrario, che nulla osta al loro permanere: è, infatti, più ragionevole ritenere che l'eventuale esclusione di una norma fondamentale come gli art. 214 e 215 c.p.c. dovesse essere esplicita"⁴5⁵. Si tratta, in sostanza, di

⁽³⁾ Vedremo, infatti, che l'autenticazione della firma digitale prevista dall'art. 16 del D.P.R. 513 rappresenta un *quid pluris* rispetto all'autenticazione tradizionale come prevista dall'art. 2703 c.c.. Cfr. par. 9 in questo capitolo.

⁴ Così L. ALBERTINI, *Sul documento informatico e sulla firma digitale (novità legislative)*, cit., p.288 ss.

⁵ In realtà questa prima argomentazione è pienamente controvertibile. Infatti, come sottolineato dal GRAZIOSI (op. cit., p.515) se il legislatore avesse voluto richiamare l'intera disciplina dell'art. 2702 c.c. avrebbe utilizzato formule diverse da quelle del citato art. 5, come ad esempio: "nei casi previsti dall'art. 2702 c.c. il documento informatico sottoscritto con firma digitale fa piena prova fino a querela di falso" ovvero "il documento informatico fa piena prova fino a querela di falso quando ricorre una delle condizioni di cui all'art. 2702 c.c.....".

applicazione dell'adagio latino “*ubi legis auctor voluit, dixit; ubi noluit, tacuit*”.

Secondariamente, si sostiene che, sancita, dalla normativa autorizzata, la piena equipollenza tra firma digitale e sottoscrizione tradizionale (art. 10 comma 2), non vi sono ragioni per negare, su un piano strettamente tecnico, la praticabilità del procedimento di verifica ai documenti informatici perché volto ad accertare (attraverso il rispetto dei criteri di formazione previsti dal regolamento) la provenienza di questi ultimi, dato che il disconoscimento ha ad oggetto l'autenticità della firma digitale. Tra l'altro, a considerarsi la scrittura privata informatica una prova precostituita al processo al pari di quella tradizionale⁽⁶⁾, ne deriverebbe l'imprescindibilità

⁽⁶⁾ Questa è la soluzione preferibile. Il documento informatico, infatti, al pari di quello tradizionale viene formato fuori e prima del processo, nel quale entra attraverso un semplice atto di esibizione o di produzione. I documenti, come insegna MANDRIOLI (*Corso di diritto processuale...*, cit., p. 141 ss.), sono, già per sé stessi, dotati dell'attitudine a produrre efficacia probatoria, sicché a produzione avvenuta, al giudice non rimane da svolgere altra attività, rispetto ad essi, se non quella del loro apprezzamento, o valutazione, ossia un'attività che già concerne la fase di decisione e non anche quella di istruzione. Le particolarità tecniche di formazione di una scrittura privata informatica hanno, però, indotto qualcuno (GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, cit., p. 510) a sussumerla sotto la categoria concettuale delle prove costituenti. Premesso che per prove costituenti devono intendersi quei mezzi di prova (es. il giuramento, la testimonianza, la confessione) che si formano soltanto nel processo e che possono essere soltanto prospettate come possibili, immaginate o preventivate (la definizione è sempre del MANDRIOLI), l'A. citato preso atto dell'ineluttabilità del necessario controllo che il giudice deve fare per verificare se la scrittura prodotta dalla parte è stata firmata con chiave valida (altrimenti ex art. 10 comma 5 D.P.R. 513 non ci sarebbe stata sottoscrizione) inquadra normativamente quest'ultimo nella previsione dell'art. 261 c.p.c. Si tratterebbe, insomma, di un esperimento giudiziario, volto a verificare, tramite ripetizione nel processo, se la verifica che la parte, produttore lo scritto, sostiene aver avuto esito positivo fuori dal processo, possa effettivamente aver dato quel risultato. Il vantaggio di questa tesi sta nella possibilità di saltare “a piè pari” il problema relativo al disconoscimento – verifica della scrittura privata informatica, perché ci si trova di fronte ad una prova formata nel processo e non precostituita ad esso. Per invalidare le certezze raggiunte in sede di istruzione rimarrebbe solo il rimedio della querela di falso (artt. 221 ss. c.p.c.). Il configurare la scrittura privata informatica come prova costituita (*rectius*: precostituita per quanto riguarda la dichiarazione documentale, costituendo riguardo alla prova della sua provenienza), tuttavia non convince. Infatti, prove costituenti sono solo quelle prospettate come possibili, immaginabili o preventivate. Ebbene, una tal definizione mal si adatta al documento informatico che è sempre e comunque precostituito al processo. Nel

del procedimento di verifica anche rispetto alla prima, poiché la *ratio* del procedimento di verifica è rinvenibile proprio nella minore forza di convincimento che queste prove hanno (proprio perché privatamente precostituite al processo) rispetto a quelle liberamente valutabili⁽⁷⁾.

In terzo luogo, si sostiene, ammettere la disapplicazione della normativa relativa al disconoscimento e alla verifica nei confronti della scrittura privata informatica, implicherebbe una palese violazione, in breve, del principio di uguaglianza delle parti nel processo. E, infatti, si argomenta che: "il procedimento di certificazione precedente al rilascio della chiave pubblica fornisce una certezza solo in ordine all'identificazione del soggetto che ha richiesto la chiave medesima, ma non consente di escludere il rischio che, successivamente al rilascio, qualcun altro utilizzi illegittimamente la chiave rilasciata al titolare. L'esistenza di questo rischio impone di considerare imprescindibile il riconoscimento del documento informatico da parte del soggetto contro il quale lo stesso è prodotto"⁽⁸⁾. Ne deriva, poi, necessariamente che "se si concepisce la verifica come ulteriore strumento difensivo concesso alla parte che ha prodotto un documento poi

caso di una dichiarazione firmata digitalmente, i termini della questione non cambiano: il giudice non deve fare altro che visualizzare il contenuto del documento. A qualificarlo prova costituenda non basta il rilievo che la firma digitale non sia dotata del requisito, proprio della firma tradizionale, della leggibilità che, anzi, abbiamo visto non appartenerle.

⁽⁷⁾ Così F. DE SANTIS, *La disciplina del documento informatico. Il commento*, cit., p.393. Anche F. DELFINI, *Forma e trasmissione del documento informatico nel reg. ex art. 15.2 L. 59/97*, cit., p.631, è orientato nello stesso senso. In particolare, facendo leva sulla piena equivalenza tra sottoscrizione tradizionale e firma digitale, l'A. sostiene che "l'art. 10 comma 2 D.P.R. 513, disponendo che la firma digitale *equivale* alla sottoscrizione prevista per gli atti e i documenti in forma scritta su supporto cartaceo, sembra richiamare l'intera disciplina in tema di sottoscrizione "convenzionale", e non già escludere la necessità del riconoscimento della sottoscrizione".

disconosciuto, l'identità di *ratio* che consente l'estensione analogica della verifica anche ai documenti all'esame sarebbe, in questa prospettiva, rappresentata dalla mera compatibilità tecnica del meccanismo processuale in rapporto all'intenzione di assicurare un ulteriore corso ad ogni documento prodotto, non assistito dalla pubblica fede, disconosciuto e, quel che più importa, verificabile⁽⁹⁾.

A parere di chi scrive, nessuna delle argomentazioni sopra riportate convincono appieno, perché foriere, in particolare la terza, di conclusioni abnormi.

Infatti, il riconoscere, come fa la dottrina sopra menzionata, la possibilità, da parte del titolare della corrispondente chiave privata, di disconoscere la firma digitale validamente apposta nonché, conseguentemente, alla parte produttrice lo scritto informatico disconosciuto di chiedere la verifica, si scontra con le caratteristiche intrinseche al sistema di firma digitale nonché con le stesse norme regolamentari che di queste caratteristiche sono espressione.

Quanto detto trova conferma nella constatazione che la firma tradizionale è espressione somatica e personale dell'individuo che l'ha apposta e quindi crea un collegamento di natura soggettiva tale da permettere alla parte contro cui sia prodotta una scrittura privata, di poter affermare o negare che quella sottoscrizione provenga effettivamente da lui, in ragione dell'alternativa fra

⁽⁸⁾ Così F. FERRARI, *La nuova disciplina del documento informatico*, cit., p. 144-148.

⁽⁹⁾ Così F. DE SANTIS, *La disciplina del documento informatico. Il commento*, cit., p.393.

autenticità o falsità del segno grafico. Se la parte contro cui viene prodotta la scrittura disconosce la sua sottoscrizione lo fa, appunto, perché eccepisce la mancanza del nesso di riferibilità del segno grafico alla propria persona e l'ordinamento, a questa eccezione, risponde facoltizzando la parte interessata ad azionare il procedimento di verifica, che in tanto ha un senso in quanto il legislatore ha riconosciuto la probabile eventualità che il *segno grafico* altrui venga contraffatto.

Tale collegamento soggettivo non si riscontra nella scrittura privata informatica, perché ad esso si sostituisce un collegamento oggettivo – verificabile – tra firma digitale e chiave privata corrispondente. Questo collegamento oggettivo, non è idoneo a dar vita all'alternativa tra autenticità e falsità del *segno digitale*.

Dimostrazione di quanto affermato è data dal fatto che la firma digitale risulterà sempre autentica indipendentemente dal fatto che la sua apposizione al documento informatico, verificato positivamente, sia posta in essere da soggetto diverso da quello che si ritiene essere presuntivamente *ex lege* il suo autore.

Questo in applicazione dei principi, precedentemente enunciati, di complementarità ed indipendenza¹⁰ della coppia di chiavi asimmetriche: ne deriva la quasi – assoluta impossibilità di contraffare una firma digitale.

¹⁰ Ribadisco che per *complementarità* delle chiavi deve intendersi la loro relazione biunivoca: l'una viene utilizzata per cifrare il testo e l'altra per decifrare il medesimo. In altri termini, il documento codificato con una delle due chiavi può essere decodificato solo con l'altra chiave, e non riutilizzando la prima. Per *indipendenza* delle chiavi deve intendersi l'impossibilità, conoscendo la chiave pubblica, di poter risalire a quella privata. Cfr. Cap. I par. 3.

Stando così le cose, viene a mancare la *ratio* stessa degli istituti del disconoscimento e della verifica, perché miranti ad accertare incontrovertibilmente la *paternità* di una scrittura, quando, invece, la verifica, se positiva, della firma digitale con la corrispondente chiave pubblica, assicura incontrovertibilmente la *titolarità*¹¹ della corrispondente chiave privata.

In breve: non si ha più paternità, bensì titolarità della firma. L'uso esclusivo della chiave privata sostituisce l'esclusività della grafia manuale.

Ne deriva che il segno digitale risulta solamente idoneo a configurare l'ipotesi di utilizzo lecito od illecito, da parte di terzi, della chiave privata con cui apporre una firma digitale, che, in entrambi i casi, corrisponderà comunque ad un *segno digitale di per sé valido ed autentico*¹².

D'altra parte, tutte le norme regolamentari relative alla firma digitale autorizzano ad opinare in tal senso.

Così, già a livello definitorio, possono trovarsi elementi a sostegno di tale tesi nel raffronto tra quanto dispone l'art. 1 lett. f) del D.P.R. 513/97 e quanto prescritto dall'art. 1 lett. a) dell'allegato tecnico al d.p.c.m. 8 febbraio 1999.

L'art. 1 lett. f) del D.P.R. 513 definisce la chiave pubblica come "l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con la

¹¹ Nello stesso senso M. ORLANDI, *L'imputazione dei testi informatici*, cit., p. 871-3 e 889. Secondo l'A. "la firma digitale è intrinsecamente incapace di restituire la prova della paternità materiale, giacché rappresenta non l'autore della digitazione bensì il titolare della digitazione ...", "... che l'autore materiale della firma (il digitatore della chiave) sia tizio o Caio nulla più rileverebbe, poiché l'oggettiva apposizione del codice digitale potrà essere in sé sufficiente per imputare la scrittura al titolare della chiave".

¹² Così F. RIZZO, *Valore giuridico ed efficacia probatoria del documento informatico*, cit., p.224

quale si *verifica* la firma digitale apposta sul documento informatico *dal titolare* delle chiavi asimmetriche...”.

A sua volta l'art. 1 lett. a) Reg. tec. individua con precisione il soggetto cui riferire il documento informatico, definendolo come “il soggetto a cui è *attribuita* la firma digitale generata con la chiave privata della coppia...”.

Queste norme, fra loro complementari creano, come rilevato da attenta dottrina¹³, una sorta di circolare riferibilità della firma digitale al titolare delle chiavi asimmetriche: la prima, infatti, attribuisce, da un lato, la firma digitale verificata positivamente con la chiave pubblica al titolare di quest'ultima; la seconda, in senso inverso, attribuisce la firma digitale al soggetto titolare della chiave privata con cui la firma digitale è stata generata.

Tali norme non fanno altro che ribadire il meccanismo di funzionamento di un sistema crittografico asimmetrico, ma dato che lo fanno a livello normativo avranno valore precettivo e non mero valore rappresentativo.

Chi viene individuato dal legislatore non è un qualsiasi potenziale utilizzatore delle chiavi private, ma un soggetto determinato, il titolare appunto, alla cui identificabilità le norme regolamentari paiono essere teleologicamente formulate.

La stessa definizione di firma digitale (art.1 lett. b)) là dove dispone che tramite la chiave pubblica si *verifica* la *provenienza* oltre che l'integrità di un documento informatico, letta in relazione alle due definizioni sopracitate, denuncia l'intenzione del legislatore di voler creare un'unica condizione

normativa (nella specie “l’esclusività dell’apparato tecnico”) che *a priori* attribuisca alla firma digitale l’efficacia probatoria di cui all’art.2702, senza la necessità che intervengano, a posteriori, quegli espedienti integrativi necessari, invece, nei confronti della firma autografa.

Una *presunzione di riferibilità*, quindi, della firma digitale al suo autore, che fa sì che quest’ultimo non possa disconoscere la prima, quando corrisponda alla chiave privata in sua esclusiva disponibilità, perché essa è giuridicamente considerata la *sua* firma.

Tra l’altro, la possibilità che potesse crearsi una dissociazione soggettiva fra il presunto sottoscrittore e il reale utilizzatore della chiave privata è stata tenuta in considerazione dal legislatore, che ha dettato tutta una serie di norme volte a garantire la reale corrispondenza tra il secondo e il sottoscrittore individuato *ex lege*, riducendo quindi ai minimi termini il rischio di verifica di una tale evenienza.

In quest’ottica vanno lette le norme relative all’attività di certificazione, volte ad assicurare un legame tra la coppia di chiavi ed un’identità soggettiva (ad esempio, oltre a quelle già citate, l’art. 4 comma 1 Reg. Tec.: “*Una coppia di chiavi può essere attribuita ad un solo titolare*”).

Un ruolo centrale assume l’art. 8 comma 4 dell’allegato tecnico al d.p.c.m. 8 febbraio 1999 che individua gli obblighi cui l’utilizzatore di una coppia di chiavi asimmetriche deve conformarsi: in particolare egli deve conservare con la massima diligenza la chiave privata e il dispositivo (di firma) che la

¹³ Così RIZZO, *Valore giuridico ed efficacia...*, cit., p. 224 nota 31.

contiene al fine di garantirne l'integrità e la massima riservatezza; conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi.

Tale norma va poi coordinata con l'art. 10 comma 4 del Reg. Tec. dedicata al "dispositivo di firma", il quale dovrà procedere all'*identificazione del titolare* prima di procedere alla generazione della firma.

Il "dispositivo di firma" viene definito dall'art. 1 lett. d) come "l'apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado *almeno* di conservare in modo protetto le chiavi private e generare al suo interno firme digitali" (presumibilmente una *smart card* protetta da un codice segreto come un PIN - analogamente a quanto avviene per le carte bancomat - o da una password).

A tutto ciò potranno aggiungersi dei dispositivi di identificazione biometrica volti a garantire ancor di più la corrispondenza soggettiva tra titolare delle chiavi e reale utilizzatore del sistema).

Pare, dunque, che il Governo, nell'emanare le norme autorizzate, abbia utilizzato la formula di cui all'art. 5 D.P.R. 513 per richiamare la sola efficacia probatoria di cui all'art. 2702 c.c. e non l'intera fattispecie astratta prevista da tale articolo, perché consapevole delle peculiarità del "nuovo strumento impersonale di imputazione soggettiva"; peculiarità che rendono

superflue, rispetto alla firma digitale, quelle condizioni normative pensate appositamente dal legislatore in relazione alla sottoscrizione autografa.

D'altra parte la verifica, positiva, della firma digitale operata dal terzo tramite la chiave pubblica corrispondente, unitamente al sistema di validazione, permette l'equiparabilità *quoad effectum* alla verifica giudiziale.

Indicazioni in tal senso sembrano provenire anche dalla relazione di accompagnamento del D.P.R. 513 là dove si afferma che "...può dirsi risolto, con l'adozione dal sistema di firma digitale, il problema della *univoca* identificazione dell'autore..." di un documento informatico.

Il giudice istruttore, peraltro, dovrà effettuare un necessario controllo al momento dell'esibizione della scrittura privata informatica, volto ad accertare la validità o meno della firma digitale¹⁴.

Controllo che non potrà essere considerato come un'istanza di verifica ai sensi dell'art. 216 c.p.c., in quanto dovrà essere effettuato ogniqualvolta venga prodotto un documento informatico e non solo a seguito di disconoscimento della controparte.

Accertamento quindi "necessario" e non, come la verifica giudiziale, solo "eventuale".

¹⁴ Accertamento *nel* processo, quest'ultimo, che non verterà sulla provenienza della scrittura privata informatica (perché immediatamente riscontrabile *fuori* dal medesimo) ma, in quanto implicante un controllo sulla legalità, sarebbe solo funzionale all'ottenimento di un titolo per la trascrizione nei registri immobiliari (che ex art. 2657 c.c. può avvenire solo in forza di sentenza, atto pubblico o di scrittura privata con sottoscrizione autenticata o accertata giudizialmente) e delle imprese (art. 2189 c.c.). Così ZAGAMI, *La firma digitale tra soggetti...*, cit., p. 908 nota 17.

Necessario controllo, in conclusione, volto ad accertare quanto la parte che produce il documento dichiara, cioè che la firma digitale è risultata valida in seguito a verifica della stessa ex art. 1 lett. c) D.P.R. 513.

Ne deriva che l'unico strumento a disposizione del convenuto per contrastare le risultanze della scrittura privata informatica prodotta dalla controparte è la querela di falso.

Tra l'altro, è dato rilevare, come la stessa dottrina sostenitrice della piena applicabilità degli istituti del disconoscimento e verifica alla scrittura privata informatica arrivasse "implicitamente" alle stesse conclusioni qui appena formulate.

Infatti, non potendo ammettere che la parte contro cui viene prodotto il documento informatico potesse semplicemente disconoscerlo invocando l'abuso - derivante dall'utilizzo illegittimo della chiave privata da parte di terzi - senza provarlo (pena l'addossare alla parte produttore un onere probatorio quasi diabolico), gli autori sopra citati si vedevano costretti a ripartire, in dispregio a quanto stabilito dall'art. 216 c.p.c., l'onere della prova quasi interamente a carico del presunto sottoscrittore¹⁵.

Sarebbe spettato a quest'ultimo, alla luce di quanto dispongono gli artt. 9 comma 1 e 10 comma 5 D.P.R. 513, fornire la prova negativa dell'insussistenza di abusi o illeciti di terzi, bastando, in sede di verifica, a chi continuasse a sostenere l'autenticità della scrittura informatica prodotta, dimostrare la validità della firma digitale, oggetto di "comparazione digitale",

producendo il relativo certificato (peraltro desumibile dalla stessa firma ex art. 7 D.P.R. 513 et art. 9 comma 2 Reg. Tec.).

Ma così opinando, sull'onda del presunto adeguamento delle disposizioni civilistiche e del codice di rito alla nuova realtà informatica, si afferma, da un lato, l'inoperabilità dell'art. 216 c.p.c. che prescrive, letteralmente, l'onere della prova a carico di chi invoca l'efficacia della scrittura privata; dall'altro, si fanno confluire tutte le ipotesi di falso¹⁶ documentale nell'oggetto della verifica operando, in sostanza, una osmosi fra due istituti che sono concettualmente distinti¹⁷ ed escludendo, di fatto, la proponibilità della querela di falso.

¹⁵ Così DELFINI, *op. cit.*, p. 631; ROGNETTA, *op. cit.*, p. 74; DE SANTIS, *op. cit.*, p.393.

¹⁶ La falsità del documento può investire il profilo *estrinseco* (ossia il documento nella sua materialità) oppure il suo *contenuto*. Nel primo caso si parla di *falsità materiale*: essa concerne la *genuinità* del documento e si può manifestare nella forma della *contraffazione* (che è data dalla formazione del documento da parte di un soggetto diverso dall'autore apparente o dalla indicazione di una data o di un luogo diversi da quelli reali), e in quella dell'*alterazione* (che è data da una modificazione di ciò che risulta dal documento dopo la sua formazione). Si parla, invece, di *falsità ideologica* quando la falsità concerne la verità del documento in quanto si sostanzia in una enunciazione falsa nel suo contenuto. Ne consegue che, di regola, le falsità ideologiche non interessano l'efficacia di prova legale del documento che investe i soli profili dell'autenticità-provenienza e non formano, quindi, oggetto di querela di falso. Tuttavia, si è notato che esse possono rilevare ai fini della querela di falso quando si tratti di *falsità ideologiche che concernono l'estrinseco* e si è dato l'esempio del notaio che attesta falsamente una dichiarazione compiuta davanti a lui (c.d. falso ideologico in atto pubblico).

¹⁷ È opinione ormai pacifica sia in dottrina (V. DENTI, voce *Querela di falso*, in *Noviss. Dig. it.*, XVI, Torino, 1969, p. 663; ID., *Querela di falso e scrittura privata*, in *Scritti in onore di Carnelutti*, VI, Padova, 1950, p. 397) che in giurisprudenza (cfr. Cass., 18 giugno 1980, n. 3880, in *Giust. Civ. Mass.*, 1980, p. 6). Infatti oggetto del giudizio di verifica è la provenienza del documento cui si ricollega in via presuntiva - si tratta di presunzione *juris tantum* - la paternità delle dichiarazioni contenute nel documento medesimo; oggetto della querela di falso è invece l'accertamento della provenienza delle dichiarazioni contenute nella scrittura che appartiene ormai incontrovertibilmente a chi l'ha sottoscritta. Apparentemente contraria la classica posizione di CARNELUTTI, *Teoria del falso*, Padova, 1935, p. 100 secondo il quale "tanto l'uno quanto l'altro di questi procedimenti hanno il medesimo oggetto: verità o falsità della prova". In realtà l'A. sosteneva la medesima posizione, antepoendo, però, nel formulare la sua definizione, la finalità (comune) cui i due procedimenti sono preordinati piuttosto che l'oggetto (diverso) su cui i due giudizi ruotano.

Al di là delle diversità riscontrabili nelle premesse iniziali, mi pare che le conclusioni, almeno per quanto riguarda il piano sostanziale, siano equivalenti a quelle raggiunte in questa sede.

4. (SEGUE) – IL C.D. PRINCIPIO DEL “NON-RIPUDIO”

Abbiamo visto, al paragrafo precedente, che l'unico mezzo a disposizione del titolare di una coppia di chiavi asimmetriche per contestare le risultanze di un documento informatico validamente “sottoscritto” è la querela di falso (art. 221 ss. c.p.c.).

La scrittura privata informatica, infatti, fa piena prova (prova legale) della paternità del documento, e presuntivamente delle dichiarazioni in esso contenute, da colui che risulta essere il titolare del dispositivo di firma, secondo le risultanze del certificato.

Con la querela di falso il titolare può contestare il fatto che altri, illecitamente, abbia apposto la firma in luogo del soggetto cui *ex lege* è attribuita la paternità del documento.

Ciò che infatti si contesta con la querela di falso, non è la provenienza del documento, ormai incontrovertibilmente accertata, *prima e fuori* del processo (in forza della presunzione di riferibilità ex art. 1 lett. f) D.P.R. 513), al momento della verifica positiva della firma digitale allo stesso apposta (ai sensi dell'art. 1 lett. c) D.P.R. 513), ma bensì la provenienza delle dichiarazioni in esso contenute.

Oggetto della querela sarà, solamente, il contenuto materiale estrinseco del documento, in quanto l'efficacia di prova legale della scrittura privata non copre anche l'intrinseco, cioè la verità del contenuto della dichiarazione¹¹.

A questo punto è necessario chiedersi se, una volta esperita con successo la querela di falso, il titolare del dispositivo di firma possa validamente opporre la non-riferibilità alla sua persona delle dichiarazioni negoziali rappresentate nel documento informatico (perché da altri abusivamente immesse nel traffico giuridico) o debba, invece, sopportare comunque le conseguenze negoziali di una dichiarazione su cui il terzo ha fatto affidamento.

Un primo indizio utile alla soluzione del problema viene fornito dall'art. 9 comma 1 D.P.R. 513, laddove viene imposto a qualsiasi utilizzatore di un sistema di chiavi asimmetriche o della firma digitale di “adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri”, sancendo così specifici obblighi di protezione dei terzi, gravanti – in forza dell'utilizzo del termine *chiunque* – e sul certificatore e sul titolare della chiave privata.

¹¹ È opinione costante in dottrina (cfr. quanto riportato al paragrafo precedente in nota 17) e giurisprudenza. Si è così statuito che rimane esclusa dall'oggetto della querela di falso, in relazione alle scritture private, la falsità ideologica (Cass. civ. 11 gennaio 1988, n. 47) e che la verità intrinseca è contestabile con ogni mezzo, senza ricorrere al giudizio di falso (Cass. Civ., 6 agosto 1987, n. 6781, in Mass. 1987). Per quanto riguarda l'oggetto esclusivo della querela di falso rispetto alla verifica (o il disconoscimento: l'oggetto rimane comunque il medesimo) è utile riportare quanto statuito da Cass., 18 giugno 1980, n. 3880, in Giust. Civ. Mass., 1980: “la querela di falso e il disconoscimento della scrittura privata sono istituti preordinati a finalità diverse e del tutto indipendenti tra loro... il secondo investe la provenienza del documento ed è volto a impedire che la scrittura acquisti l'efficacia di una scrittura legalmente riconosciuta, negando l'autenticità della sottoscrizione della scrittura, onde impedire che all'apparente sottoscrittore di essa venga imputata la dichiarazione sottoscritta; mentre allorché sia accertata l'autenticità della sottoscrizione, chi voglia contestare la provenienza delle dichiarazioni contenute nella scrittura da colui che, ormai incontrovertibilmente, l'ha sottoscritta, ha l'onere di proporre querela di falso”.

Quanto, poi, questo obbligo di protezione dei terzi vincoli il titolare della chiave privata alla dichiarazione digitalmente firmata viene specificato da altra disposizione regolamentare.

L'art. 10 comma 5 del D.P.R. 513/97, infatti, così dispone: *“L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate”*.

Sembra dunque che il legislatore, nello stabilire le conseguenze che ricadono su colui che risulta autore di una firma digitale, dopo la verifica del relativo certificato, abbia optato per un regime di quasi-assoluta vincolatività, senza possibilità di eccepire, da parte del titolare della coppia di chiavi, l'incolpevole falsità della firma.

Questo in virtù del particolare regime di attribuzione intrinseco alla firma digitale, che vincola in maniera pressoché assoluta il soggetto cui è univocamente riferibile.

Gli unici casi, infatti, in cui tale esclusivo e formale collegamento viene meno sono, da un lato, il caso in cui sia pubblicato, ad opera del certificatore, il provvedimento di sospensione o di revoca del certificato e, dall'altro, il caso in cui il titolare delle chiavi crittografiche fornisca la prova che la revoca o la sospensione, comunque motivate e ancorché non pubblicate, erano già a conoscenza delle parti interessate.

In questi soli casi, quindi, il titolare della firma digitale sarebbe liberato e dalle conseguenze negoziali discendenti dal documento informatico e dall'eventuale obbligo risarcitorio su di lui gravante in base all'art. 9 comma 1 del D.P.R. 513.

Questo perché si tratterebbe di *circostanze oggettive e conoscibili*, che, quindi, escludono l'affidamento dei destinatari.

In ogni altro caso, l'abuso, pur provato tramite querela di falso, non potrebbe essere opposto ai terzi dal titolare delle chiavi asimmetriche.

Questo particolare regime di responsabilità gravante sull'utilizzatore di un sistema di firma digitale, esplicita quella che è una caratteristica fondamentale della medesima, ovvero, il quasi suo assoluto "non-ripudio"².

Due sono i principi fondanti l'intero sistema di funzionamento della firma digitale: quello della "tutela dell'affidamento dei terzi"³ e quello di "autoresponsabilità"⁴, ripensati, però, in modo più rigoroso rispetto al ruolo che viene loro assegnato tradizionalmente⁵.

² Nel dibattito internazionale si parla di "repudiation", con riferimento alla possibilità di respingere l'imputabilità giuridica del documento informatico firmato digitalmente con la chiave privata del soggetto che accerta l'abusivo utilizzo della stessa.

³ Molto si è scritto intorno alla portata precettiva del principio dell'affidamento. Fra i tanti vedansi V. PIETROBON, *Errore, volontà e affidamento nel negozio giuridico*, Padova, 1990; G. MARINI, *Promessa e affidamento nel diritto dei contratti*, Napoli, 1995; E. BETTI, *Teoria generale del negozio giuridico*, in Tratt. dir. civ. diretto da Vassalli, XV, 2, Torino, 1960.

⁴ Cfr. PUGLIATTI, *Autoresponsabilità*, in Enc. dir., IV, Milano, 1959, p. 452 ss.; SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1966.

⁵ Per l'applicazione dei principi di affidamento e autoresponsabilità alla fattispecie del documento e contratto informatico vedi MIRABELLI, *Contratto tra terminali e documento elettronico*, in Riv. Not., 1986, p. 769 ss.; DI GIOVANNI, *Il contratto concluso mediante computer alla luce della Convenzione di Roma sulla legge applicabile alle obbligazioni contrattuali del 19 giugno 1980*, in Dir. Comm. Internaz., 1983; A. M. GAMBINO, *L'accordo telematico*, Milano, 1997; GENTILI, *Documento informatico e tutela dell'affidamento*, in riv. dir. civ., II, 1998.

Secondo quest'ultimo, chi immette o dà causa all'immissione di dichiarazioni negoziali nel traffico giuridico è assoggettato alle conseguenze di esse secondo il loro *obbiettivo* significato. Aggiungasi che il dichiarante rimane impegnato dalle sue dichiarazioni o dalle dichiarazioni a cui abbia dato causa a prescindere da una valutazione della sua condotta in termini di colpa: ne deriva che sul titolare di una coppia di chiavi asimmetriche grava il rischio di una dichiarazione non conforme alla sua volontà reale e, oltre, di una dichiarazione non voluta.

Questa soluzione, che privilegia l'affidamento rispetto alla tutela dell'integrità del consenso, risponde all'esigenza di certezza del traffico giuridico, quanto mai sentita nell'ambito dei rapporti commerciali.

Specifiche norme si ispirano a tale regola di autoresponsabilità in funzione di tutela dell'affidamento.

Così, ad esempio, il già citato art. 8 comma 4 reg. tec., per cui è fatto *onere* al soggetto titolare della chiave privata di denunciare alla competente Autorità ogni evento (furto, smarrimento, ecc.) che possa comportare il pericolo di utilizzo della chiave stessa da parte di altri, e quindi chiederne la revoca o la sospensione³⁶. In mancanza di tale diligenza, verrà imputata al soggetto

³⁶ Correlativamente al certificatore viene fatto obbligo ex art. 9 lett. h-i) D.P.R. 513 di procedere tempestivamente alla revoca o sospensione del certificato e di dare immediata pubblicità a questi "incidenti" (per utilizzare un'espressione di M. CAMMARATA, *Sospensione, revoca e altri incidenti*, in *Le regole tecniche per la firma digitale*, 10, 2 giugno 1999, all'indirizzo <http://www.interlex.it>). Il regime di responsabilità gravante sul certificatore deve intendersi in maniera molto rigorosa: prova ne è data dall'utilizzazione da parte delle norme autorizzate degli avverbi "tempestivamente" e "immediatamente" le quali individuano la misura di diligenza richiesta al certificatore medesimo a cui è richiesta un'azione positiva computabile non in settimane o giorni ma in ore se non, addirittura, in secondi. Sarà il contesto operativo a suggerire la migliore politica da adottare (si pensi a quante transazioni bancarie avvengono ogni secondo). Così M.

titolare ogni attività documentale posta in essere utilizzando la chiave suddetta.

Specularmente a quanto più sopra enunciato, il principio dell'affidamento informa che chi emette una dichiarazione negoziale o tiene un comportamento che abbia un significato negoziale o si avvale di altri per comunicare la sua dichiarazione, suscita nel destinatario l'affidamento che l'atto sia serio e conforme al suo obiettivo significato, secondo la normale esplicazione dell'attività negoziale. Ne deriva che, di regola, l'esigenza di tutela dell'affidamento supera l'esigenza di tutela del dichiarante perché la rilevanza, rispetto ai terzi, delle deficienze occulte della dichiarazione negoziale pregiudicherebbe la certezza del commercio giuridico.

L'unico limite che, tradizionalmente, veniva riconosciuto all'operatività di questo principio e, conseguentemente, a quello dell'autoresponsabilità, risiedeva nella conoscenza o nella possibile conoscenza che il terzo, usando la media diligenza, potesse avere della non autenticità della dichiarazione proveniente dalla controparte (ad es.: il destinatario sa, o avrebbe dovuto sapere, che la dichiarazione è stata erroneamente trasmessa).

Non era ritenuto bastevole, infatti, per l'operatività del principio, che il destinatario facesse affidamento su una realtà negoziale inesistente se questa non era riferibile alla parte: il danno derivante da tale evento doveva,

MACCARATA e E. MACCARONE, *Il ruolo del certificatore*, in *Introduzione al ruolo del certificatore*, in <http://www.interlex.it>.

piuttosto, rimanere nella sfera di colui che lo aveva subito, non potendo essere addossato al soggetto rimasto estraneo alla vicenda.

Questo correttivo all'operatività del principio dell'affidamento non trova tuttavia cittadinanza nell'impianto regolamentare disciplinante la firma digitale, in virtù di quanto disposto dagli artt. 9 comma 1 et 10 comma 5 del D.P.R. 513.

Il terzo, infatti, non ha, di regola, alcuna possibilità di conoscere fisicamente la controparte: ne deriva che non può essergli richiesto, anche in applicazione di quanto disposto dagli artt. 1337-38 c.c., altro comportamento se non il soddisfacimento dell'onere relativo alla consultazione del registro dei certificati, onde verificare la perdurante validità della chiave privata con cui è stata firmata l'eventuale proposta contrattuale.

Opera, quindi, il più penetrante principio dell'*apparenza imputabile*, in base al quale viene giustificata la sopportazione del rischio, incombente sul titolare delle chiavi asimmetriche, di un'utilizzazione abusiva della firma digitale.

Tale principio, riconosciuto solo eccezionalmente dal codice civile (vedi, ad es., l'art. 534 c.c. sull'erede apparente; l'art. 1189 c.c. sull'apparente legittimato a ricevere la prestazione; l'art. 1153 sull'acquisto di cose mobili *a non-domino*, ecc.), è il frutto dell'elaborazione giurisprudenziale¹⁷ e può

¹⁷ Il principio dell'apparenza imputabile, da intendersi come la regola secondo cui chi crea l'apparenza di una condizione di diritto o di fatto è assoggettato alle conseguenze di tale condizione nei confronti di chi vi abbia fatto ragionevole affidamento, è stato così specificato da Cass. 30 maggio 1969, n. 1934: "del principio dell'apparenza il terzo può giovare quando egli, di fronte ad uno stato di fatto non corrispondente a quello di diritto, abbia agito con il ragionevole

ormai considerarsi di diritto effettivo. Il principio dell'apparenza imputabile postula, dunque, una particolare forma di autoresponsabilità del soggetto che dà causa all'affidamento dei terzi sulla riferibilità ad esso di atti e rapporti.

Ciò che rileva, per l'operatività di questo principio, non è tanto la buona fede del terzo (che si presume: arg. ex. 1147 c.c.), quanto l'imputazione causale dell'apparenza al soggetto che abbia posto in essere (ad es., cedendo ad altri il dispositivo di firma e i relativi codici di abilitazione) o reso possibile (ad es., non dando immediata comunicazione al certificatore dello smarrimento della chiave privata) il verificarsi della situazione apparente.

Sulla base di quanto esposto e facendo leva su precise indicazioni regolamentari (artt. 9 e 10 del D.P.R. 513) certa dottrina³⁸ ha affermato che “colui che entra nel commercio giuridico avvalendosi della chiave elettronica, dà causa alle situazioni di apparenza create mediante l'abusiva utilizzazione di tale chiave perché comunque si è avvalso di uno strumento suscettibile di creare falsi affidamenti: l'imputazione della dichiarazione al titolare della chiave abusivamente utilizzata risulta allora conforme al principio dell'apparenza imputabile”.

convincimento, derivante da errore scusabile, che lo stato di fatto rispecchi la realtà giuridica, così che, per aver fatto affidamento su una situazione giuridica non vera, ma solo apparente, e per essersi comportato in aderenza alla stessa, abbia diritto di contare sulla manifestazione apparente non conforme alla realtà. Sono, cioè, necessarie in ogni singolo caso la buona fede del terzo e la ragionevolezza dell'affidamento, non essendo invocabile il principio anzidetto da chi versi in colpa per aver omesso di accertare, in contrasto con la stessa legge e con le norme di comune prudenza, la realtà delle cose, affidandosi alla mera apparenza”.

³⁸ Così C. MASSIMO BIANCA, *I contratti digitali*, in *Studium iuris*, II, 1998, p.1037 et 1038.

Neanche rivelerebbero gli stati soggettivi del titolare delle chiavi (ad es. tutta la disciplina dell'errore ex artt. 1427-1433 c.c.) invalidanti il negozio perché, al di fuori della limitata *pubblicità di fatto*, per cui è consentito provare (con l'onere della prova a carico del revocante o di chi chiede la sospensione) che la revoca o sospensione era già a conoscenza delle parti interessate, anche in mancanza, o prima, della necessaria pubblicazione, l'errore come "l'uso abusivo della chiave non incide sulla validità del documento, la quale è data *esclusivamente* dalla sua conformità alle prescrizioni di legge (art. 2 D.P.R. 513)".

Come dire: "*eius commoda et eius, ibi, incommoda*".

Una tale interpretazione, seppur aderente alle prescrizioni regolamentari, se accolta, rischierebbe di inficiare l'effettività di regole fondamentali del nostro ordinamento, che impongono che esso si perfezioni in forza della presenza del "consenso", legittimamente manifestato, delle parti e che richiedono nei confronti dell'atto in genere la sussistenza della "volontà" di chi ne è l'autore⁹⁹.

A parere di chi scrive, deve preferirsi un'interpretazione meno restrittiva della formula rinvenibile all'art. 2 del D.P.R. 513, la quale dichiarando "validi e rilevanti a tutti gli effetti di legge" i contratti formati in via telematica va riferita al documento e solo di riflesso ai negozi ivi

⁹⁹ Così RIZZO, *Valore giuridico ed efficacia probatoria del documento informatico*, cit., p. 238.

rappresentati che quindi soggiaceranno alle regole comuni in tema di invalidità del contratto¹⁰.

Nella specie, gli effetti negoziali derivanti da un documento informatico abusivamente firmato non potranno essere imputati alla parte che riesca a dimostrare, tramite querela di falso, la sua estraneità all'emissione della dichiarazione negoziale (proposta o accettazione che sia) nel traffico giuridico.

Ne consegue che il titolare di una chiave privata usata abusivamente che dimostri, in seguito a querela di falso, l'illecito utilizzo della stessa, sarà liberato dagli effetti dell'atto ma non dagli obblighi risarcitori su di lui gravanti per il disposto dell'art. 9 D.P.R. 513.

Il richiamo che l'art. 9 cit. fa alla predisposizione di "tutte le misure organizzative e tecniche idonee ad evitare danno ad altri" ha portato la dottrina ad inquadrare questa locuzione nell'ambito dell'art. 2050 c.c., come forma di *responsabilità oggettiva* gravante e sul certificatore e sul titolare delle chiavi asimmetriche per il danno che il terzo possa aver subito facendo affidamento sulle risultanze del certificato.

In particolare al terzo basterà, secondo i principi generali, fornire la prova del danno ricevuto e del nesso di causalità tra danno ed esercizio dell'attività pericolosa. Spetterà alla controparte dimostrare l'inevitabilità del danno pur in presenza di tutte le cautele previste dall'art. 9 del D.P.R. 513.

¹⁰ Così BIANCA, *Diritto civile*, III, *Il contratto*, Milano, 2000, p. 310.

Tuttavia per espresso disposto dell'art. 2056 c.c. a sua volta richiamato dall'art. 2050 c.c. il risarcimento non sarà dovuto per i danni che il terzo danneggiato avrebbe potuto evitare usando l'ordinaria diligenza: ne deriva che se il terzo conosceva o era in grado di conoscere l'effettivo utilizzatore del dispositivo di firma come persona diversa dal titolare delle chiavi asimmetriche nulla gli sarà più dovuto (arg. ex art. 1227 c.c.). La prova della mala fede o della colpa del terzo incomberà sul titolare una volta che il terzo abbia dimostrato il nesso di causalità.

La responsabilità aquiliana del certificatore pare potersi invocare solo in caso di non tempestiva pubblicazione della revoca o sospensione del relativo certificato, rimanendo ogni altra ipotesi risarcitoria in capo al titolare della chiave privata¹¹¹.

Soluzione quest'ultima assai severa, in funzione del massimo affidamento dei terzi, che ha portato la dottrina ad auspicare l'intervento del legislatore per la previsione di una funzione assicurativa in capo al certificatore, nei casi in cui non venga identificato l'usurpatore e il certificatore provi la sua mancanza di

¹¹¹ *Quid iuris* nel caso in cui un soggetto ignaro si veda attribuita una coppia di chiavi da un certificatore disonesto, con la quale il reale possessore firma atti e contratti a suo nome? A prima vista al titolare della coppia di chiavi che non riuscisse a dimostrare l'abuso, con querela di falso, dovuto a falsa certificazione dovrebbero essere accolte tutte le conseguenze giuridiche degli atti posti in essere dall'usurpatore. Un falso certificato, infatti, pregiudica tutto il sistema sul nascere e le conseguenze derivanti da un errore o, peggio, abuso della posizione di terzo imparziale da parte del certificatore potrebbero essere catastrofiche. A ben vedere, però, una soluzione può trovarsi nella combinata lettura dell'art. 9 comma 2 lett. a) del D.P.R. 513 ("il certificatore è tenuto ad identificare con certezza la persona che fa richiesta della certificazione") e dell'art. 22 comma 1 del Reg. tec.. Quest'ultimo infatti obbliga il certificatore a conservare per 10 anni la richiesta scritta di registrazione. Il giudice dovrebbe ordinare l'esibizione e su questo documento si svolgerebbe la verifica: con una perizia calligrafica, nel caso di richiesta redatta a mano, oppure con il controllo presso altro certificatore nel caso di richiesta avanzata con documento informatico. Il tutto sarà ricostruibile dal giornale di controllo previsto dall'art. 47 dell'All. Tec. al d.p.c.m. 8 febbraio

colpa, analogamente a quanto disposto in relazione alle società emittenti carte di credito, con un limite massimo di responsabilità per l'utente¹².

Un'ultima annotazione: esperita con successo la querela di falso, secondo l'impostazione fin qui seguita, non si produrrà alcun effetto negoziale in capo al titolare delle chiavi asimmetriche. Ma una volta identificato l'usurpatore – ipotesi alquanto improbabile nel campo della contrattazione telematica, che è per definizione una contrattazione tra assenti – potrà dirsi che quest'ultimo risulterà obbligato per gli effetti negoziali scaturenti dal contratto da lui firmato *sotto* nome altrui?

La soluzione non pare agevole, ma sembra possa darsi soluzione positiva al quesito sulla base della considerazione che a prevalere debba essere comunque il principio di conservazione del contratto (*latu sensu* inteso), considerato che, da un lato, l'usurpazione del nome altrui non pregiudica, in astratto, la possibilità dell'esatta identificazione del contraente "reale" e che, identificato quest'ultimo, non ci sarebbero motivi per ritenere nullo un contratto che soddisfa tutti i requisiti di cui all'art. 1325 c.c., dall'altro.

Come sostenuto da Piazza¹³, dato che le modalità di individuazione della parte rientrano nell'oggetto del negozio e che sono comunque validi i negozi

1999. Così M. CAMMARATA in risposta ad un quesito posto, all'indirizzo <http://www.interlex.it>.

¹² Così ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica"*, cit., p.920 nota n. 71.

¹³ PIAZZA, *L'identificazione del soggetto del negozio giuridico*, Napoli, 1968. Bisogna però precisare che tale soluzione è minoritaria e che lo stesso A. come anche la dottrina maggioritaria (cfr. per tutti ORLANDI, *La paternità delle scritture*, cit., sez. II, capp. IV-VI e A. M. GAMBINO, *L'accordo telematico*, Milano, 1997, p. 227 ss.) preferiscono ricondurre la fattispecie, con tutte le dovute difficoltà interpretative del caso, allo schema della rappresentanza indiretta perché ritenuta più

con soggetto non determinato ma però *determinabile* sulla base della legittimità della categoria dei negozi *per relationem*, potrebbe dirsi che i negozi compiuti *sotto* nome altrui non sono nemmeno ad oggetto determinabile bensì ad oggetto pienamente determinato, vertendosi solamente attorno ad una questione di interpretazione che ha come oggetto il disposto dell'art. 625 c.c.¹⁴, espressione di un principio generale.

Ovviamente, deve essere mantenuta ferma la possibilità per il terzo, nel caso di contratti personali, di poter fare valere l'errore sull'identità o sulle qualità dell'usurpatore. Errore che, secondo quanto stabilito dall'art. 1429 c.c., deve essere essenziale cioè tale che il terzo non avrebbe contrattato se non con il titolare delle chiavi asimmetriche, essendo stata l'identità personale di quest'ultimo determinante del consenso secondo criteri di normalità

praticabile. Si afferma così che "la sottoscrizione apocrifa (apposta da persona diversa da quella risultante dal nome sottoscritto) non è altro che una *contemplatio domini* non autorizzata, e produce i medesimi effetti di ogni altra spendita del nome: il diritto potestativo del contemplato alla ratifica dell'atto. Il *falsus procurator* e l'usurpatore del nome altrui si presentano come ipotesi omologhe di difetto di potere: il negozio concluso da un soggetto diverso da chi appare come titolare, presenta il requisito negativo del difetto di un potere rappresentativo" (ORLANDI, op. cit.).

¹⁴ L'art. 605 c.c. rubricato "Erronea indicazione dell'erede o del legatario o della cosa che forma oggetto della disposizione" così recita al primo comma: "*Se la persona dell'erede o del legatario è stata erroneamente indicata, la disposizione ha effetto, quando dal contesto del testamento o altrimenti risulta in modo non equivoco quale persona il testatore voleva nominare*".

5. L'ART. 60 DEL D.P.C.M. 8 FEBBRAIO 1999

Fra tutte le norme componenti il titolo III del Reg. Tec. (“Regole per la validazione temporale e per la protezione dei documenti informatici”), l’art. 60 assume un’importanza fondamentale.

Rubricato “Estensione della validità del documento informatico”, l’articolo in esame così dispone:

- 1. La validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite di validità della chiave di sottoscrizione, può essere estesa mediante l’associazione di una o più marche temporali.*
- 2. Prima della scadenza della marca temporale, il periodo di validità può essere ulteriormente esteso associando una nuova marca all’evidenza informatica costituita dal documento iniziale, dalla relativa firma e dalle marche temporali già ad esso associate.*
- 3. La presenza di una marca temporale valida associata ad un documento informatico secondo quanto previsto dal comma 2, garantisce la validità del documento anche in caso di compromissione della chiave di sottoscrizione, purché la marca temporale sia stata generata antecedentemente a tale evento.*

Prima di affrontare i problemi interpretativi sollevati da tale norma, appare, preliminarmente, opportuno approfondire il concetto di “validazione temporale” definito dal legislatore all’art. 1 lett. i) del D.P.R. 513 come “il

risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi”.

Com'è noto, la data in diritto rileva a più fini: individuare il momento in cui si è concluso un negozio giuridico, in cui deve eseguirsi una prestazione o dal quale decorre un termine e si può esercitare un diritto e così via. Essa può definirsi, in termini generali, come la proposizione che indica il tempo e il luogo in cui un certo fatto è avvenuto e, in particolare, quale elemento identificativo del documento, come l'indicazione di tempo e di luogo in cui è stata posta in essere l'attività di documentazione¹[□].

In questa seconda accezione la data consta, precisamente, dell'indicazione del giorno, del mese e dell'anno. Nel concetto di data, in senso ampio, rientra altresì l'indicazione del luogo in cui il documento è stato formato.

La data è un elemento essenziale dell'atto pubblico, mentre non costituisce elemento essenziale della scrittura privata.

Relativamente a quest'ultima, occorre puntualizzare che essa non è un elemento costitutivo necessario né della dichiarazione emessa in forma scritta, né della prova documentale della medesima. Sotto il profilo probatorio, la data riceve dal codice civile una regolamentazione diversa rispetto agli altri elementi rappresentativi del documento. In relazione ai rapporti fra le parti essa è interamente assoggettata all'art. 2702 c.c. (*tra le parti* si considera vera fino a prova contraria la data che appare dal documento); quanto, invece, ai rapporti tra le parti del rapporto sostanziale

documentato e i terzi, vigono regole particolari: quando la data non appare dall'autenticazione della firma, ottiene la certezza di fronte ai terzi con la registrazione dell'atto fatta all'ufficio del registro; oppure la data sarà certa come conseguenza di qualche altro fatto (morte del sottoscrittore o sua impossibilità fisica di firmare, o altro) dal quale si deduca che la formazione dell'atto avvenne prima di un certo giorno (art. 2704 c.c.)¹².

Nel sistema di crittografia asimmetrica i documenti si trasmettono per via telematica; sorge quindi il problema di accertare il momento in cui avviene la loro trasmissione, in modo tale da acquisire la relativa prova, anche al fine dell'opponibilità ai terzi (è principio generale, infatti, che rispetto a questi ultimi la data svolge un ruolo fondamentale nel determinare la priorità di acquisto di un diritto: la regola è quella del "*prior in tempore potior in iure*", secondo la quale il diritto è acquistato da chi ha stipulato il negozio avente data certa anteriore).

A ciò provvede proprio il servizio di validazione temporale, svolto dai certificatori¹³, consistente nell'apposizione di una marca temporale - che altro non è che il sigillo digitale apposto dal certificatore al documento con

¹² Così CARNELUTTI, voce *Documento (teoria moderna)*, in *Noviss. Dig. it.*, VI, Torino, 1975, p. 87.

¹² Per i problemi applicativi dell'art. 2704, si veda DOLMETTA, *La data certa*, Milano, 1986 e VERDE, voce *Prova documentale*, (dir. proc. civ.), Enc. Giur. Trecc., Roma, p.11.

¹³ Il D.P.R. 513, come anche il d.p.c.m. 8 febbraio 1999, non definiscono in maniera esplicita il soggetto deputato a svolgere il servizio di validazione temporale. Potrebbe, quindi, essere la stessa Autorità di Certificazione a svolgere il servizio di *time stamping*, dato che si deve trattare comunque di una *Trusted Third Part*.

un'apposita chiave privata di marcatura temporale³⁴ - avente la funzione di dare una data certa al documento informatico³⁵. La procedura corrisponde, in sostanza, a quella definita di *time stamping*: il mittente prima di inviare la sua proposta contrattuale informatica al destinatario e precisamente, ex art. 12 D.P.R. 513, all'indirizzo elettronico da questi dichiarato (producendo, quindi, gli effetti di cui all'art. 1335 c.c.), provvederà ad inviare il documento da "timbrare" ad un indirizzo elettronico, cui corrisponde il computer del soggetto che effettuerà il servizio di marcatura temporale indicato, con le modalità stabilite dal certificatore presso cui è registrato (art. 58, comma 1, d.p.c.m. 8 febbraio 1999)³⁶.

³⁴ Per la validazione temporale si utilizzano apposite chiavi, che l'allegato tecnico (art. 4 comma 4) definisce "chiavi di marcatura temporale", destinate appunto alla generazione e verifica delle marche temporali. La chiave pubblica di marcatura temporale verrà pubblicata, analogamente a quanto avviene per le chiavi di sottoscrizione e certificazione, in appositi elenchi pubblici consultabili *on-line*.

³⁵ La marca temporale, quindi, non è altro che una sequenza di simboli binari che realizza il servizio di *time stamping*. Stabilisce, infatti, l'art. 52 Reg. tec. che "una evidenza informatica (leggi: *file* di testo, suoni o immagini) è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi". Il successivo art. 53, al comma 1 stabilisce, poi, il contenuto minimo necessario di ciascuna marca temporale: essa, deve contenere: l'identificativo del mittente; il numero di serie della marca temporale apposto al *file* in questione; l'algoritmo di sottoscrizione della marca temporale; l'identificativo del certificato relativo alla chiave di verifica della marca; data e ora di generazione della marca; l'identificativo dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale; il valore dell'impronta dell'evidenza informatica.

³⁶ L'art. 12 del D.P.R. 513, rubricato "Trasmissione del documento", così dispone: "1. *Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato*. 2. *La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente regolamento e alle regole tecniche di cui all'art. 3, sono opponibili ai terzi*. 3. *La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge*". Il precedente art. 11 estende, ai contratti informatici sottoscritti digitalmente, l'applicabilità del d.lgs. 15 gennaio 1992, n. 50. Ora, come è dato rilevare anche dalla Relazione di accompagnamento al D.P.R. 513, l'art. 12 prevede innanzitutto che il destinatario di una proposta contrattuale informatica dichiari il proprio indirizzo elettronico, analogamente a quanto si verifica per una spedizione postale effettuata ad un indirizzo dichiarato o eletto dal destinatario. La data e l'ora di spedizione sono opponibili ai terzi *soltanto* se la spedizione è effettuata in conformità alle disposizioni regolamentari, in particolare quelle relative al titolo III dell'Alleg. Tec. al d.p.c.m. 8 febbraio 1999. Quello che importa qui sottolineare, è che nei

Munito di data certa, il documento in oggetto perverrà, dunque, al destinatario, il quale, volendo accertare oltre che la paternità e l'integrità della proposta informatica pervenutagli anche avere un riscontro sicuro sul momento in cui esso è stato trasmesso, non dovrà fare altro che applicare l'abituale procedimento di verifica alla firma digitale, con la corrispondente chiave pubblica di marcatura temporale, dell'ente preposto al servizio di controllo temporale.

È importante notare che la validazione temporale, così come concepita dal legislatore nostrano, fa sì che la data di un documento informatico non risulti soggetta alla disciplina dell'art. 2704 c.c., ma assuma efficacia di piena prova sia nei rapporti tra le parti, che in quelli tra queste ultime e i terzi: sostanzialmente, si verifica l'effetto civilistico della registrazione degli atti

confronti del destinatario (e sempre che il mittente sia stato rispettoso delle prescrizioni regolamentari) si crea una presunzione di conoscibilità, analogamente a quanto dispone l'art. 1335 c.c., norma cardine in materia di trasmissione delle dichiarazioni contrattuali, che deve ritenersi sicuramente applicabile alla fattispecie in esame. Dico "presunzione di conoscibilità" e non "di conoscenza", perché, in sede di esegesi dell'art. 1335, pare preferibile la tesi del RAVAZZONI (*La formazione del contratto. I. Le fasi del procedimento*, Milano, 1966, p. 326-9) secondo cui l'articolo in questione evoca una duplice presunzione: con l'arrivo all'indirizzo la dichiarazione si reputa conoscibile - prima presunzione, opponibile -, ma, una volta divenuta conoscibile, si reputa conosciuta - seconda presunzione, assoluta - (cfr. per la tesi, maggioritaria, della sola presunzione di conoscenza R. SCOGNAMIGLIO, *Dei contratti in generale (artt. 1321 - 1469)*, in Commentario del codice civile a cura di SCIALOJA e BRANCA, Bologna - Roma, 1970, p. 181 -2). Ha suscitato, poi, perplessità in dottrina il secondo comma dell'art.12 ove parla di opponibilità ai terzi della data e ora di formazione del documento informatico, oltre alla trasmissione e ricezione dello stesso. Infatti, come rilevato da ALBERTINI (*op. cit.*, p. 300) l'inciso relativo alla formazione del documento informatico si rivela un fuor di luogo, dal momento che le dichiarazioni documentali assumono rilievo nel traffico giuridico quando, oltre ad essere state "espresse" (per usare la terminologia dei fautori della "Teoria analitica della dichiarazione": cfr. P. SCHLESINGER, voce *Dichiarazione (teoria generale)*, in Enc. Dir., XII, Milano, 1964, p. 374 ss.), vengono anche "emesse", cioè sia avvenuto il distacco dall'autore essendo state inviate ai terzi. Per quanto riguarda, infine, il disposto del secondo comma dell'art. 11 del D.P.R. 513, il richiamo all'applicabilità alle contrattazioni telematiche di quanto disposto dal d.lgs n.50 del 1992, relativo alla disciplina dei contratti negoziati fuori dei locali commerciali, deve ritenersi del tutto pleonastico. Già l'art. 9 del d.lgs. citato dispone, infatti, che "*le disposizioni del presente decreto si applicano anche ... ai contratti conclusi mediante l'uso di strumenti informatici e telematici*".

già svolta dall'ufficio del registro (arg. ex art. 2704 c.c. e art. 18 D.P.R. 131/86).

Come rilevato da Zagami⁷⁷, l'unico caso in cui potrebbe operare l'art. 2704 c.c. si ha quando un documento informatico sottoscritto digitalmente non sia stato sottoposto a validazione temporale o autenticazione ex art. 16 D.P.R. 513: in questi casi, l'accertamento dell'antiorità della data nelle ipotesi di "morte o sopravvenuta impossibilità fisica a sottoscrivere" di cui all'art. 2704 c.c., sarà consentito solo fino a quando non è scaduta, revocata o sospesa la relativa chiave (il che è ovvio, considerato che in presenza di questi "accidenti" le chiavi di sottoscrizione non darebbero più alcuna garanzia circa la genuinità e l'autenticità della scrittura privata informatica di cui si voglia stabilire con certezza la data).

Venendo ora a trattare quello che è l'argomento specifico di questo paragrafo, nella specie l'art. 60 del d.p.c.m. 8 febbraio 1999, si può fin d'ora dire che una lettura poco attenta, unita ad un'interpretazione letterale del medesimo, porterebbe a conclusioni giuridicamente illogiche e congruenti.

L'articolo in esame dispone, in breve, che nel caso di documenti informatici i cui effetti si protragano nel tempo oltre il limite di validità della chiave di sottoscrizione (la quale dipenderà dalla validità del certificato relativo alla

⁷⁷ ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica"*, cit., p. 917-8. Sostiene la diversità della data digitale rispetto a quella tradizionale, limitatamente all'indicazione oraria ROGNETTA, *op. cit.*, p. 50; limitatamente all'indicazione del luogo ALBERTINI, *op. cit.*, p. 300. In dottrina si è sostenuto che l'opponibilità ai terzi della data e dell'orario, li obblighi ad assumersi l'onere di provare la fallacia e il malfunzionamento del sistema: così M. MICCOLI, *Il commercio telematico: una nuova realtà nel campo del diritto*, in *Diritto e Impresa*, III, 1997, p. 487.

corrispondente chiave pubblica, in ogni caso non superiore a tre anni ex art.1 lett. h) D.P.R. 513), è possibile estenderne la validità mediante l'apposizione di una marca temporale. Ulteriore validazione temporale che dovrà, comunque, operarsi prima della scadenza della marca temporale precedentemente apposta all'evidenza informatica e, a maggior ragione, prima della compromissione delle chiavi di sottoscrizione (sospensione e revoca).

Nell'articolo in esame si parla di "validità". Com'è noto, il termine validità indica, in termini generali, la rispondenza di un fatto o di un atto ai requisiti previsti dall'ordinamento per cui quel fatto o atto possa qualificarsi come giuridico. In particolare, la validità indica la regolarità del contratto quando questo sia dotato di tutti i requisiti previsti dall'art. 1325 c.c. e cioè: l'accordo delle parti; la causa; l'oggetto; la forma, quando risulta che è prescritta dalla legge sotto pena di nullità. L'invalidità del contratto è la risultante della mancanza di uno, o più, tra i sopracitati requisiti al momento perfezionativo dell'accordo contrattuale.

L'efficacia del contratto attiene, invece, al prodursi degli *effetti* giuridici propri del regolamento negoziale. Affermato, preliminarmente, che, di regola, un contratto valido è in quanto tale anche efficace, è, tuttavia, bene precisare che l'invalidità del contratto non comporta sempre la sua inefficacia: al riguardo occorre infatti distinguere tra nullità (artt. 1418 ss. c.c.) e annullabilità (artt. 1425 ss. c.c.) del medesimo. Il contratto nullo è *definitivamente* inefficace *ab origine*; il contratto, annullabile, invece, è

efficace, e cioè produttivo dei suoi effetti, fino a quando non intervenga un'eventuale sentenza di annullamento. Riassumendo: validità e invalidità sono qualifiche attribuite ad un determinato fenomeno nel momento in cui esso, rispettivamente, contenga o non contenga gli elementi previsti dall'ordinamento per essere considerato giuridicamente esistente od inesistente.

L'art. 2 del D.P.R. 513 sancisce la validità e rilevanza a tutti gli effetti di legge del documento informatico rispettoso dei requisiti previsti dal regolamento medesimo, operando una distinzione fra documenti firmati digitalmente e documenti sprovvisti del “segno” digitale, in funzione della differente efficacia sostanziale e probatoria che gli è riconosciuta; non sono stati, però, indicati i requisiti cui deve partecipare il documento informatico non sottoscritto digitalmente, di modo che la dottrina si è vista costretta ad individuarli in via differenziale rispetto ai documenti informatici del primo tipo.

L'articolo 60 del d.p.c.m. 8 febbraio 1999 parla di “estensione” della validità del documento informatico tramite l'apposizione delle marche temporali.

Fino all'emanazione del d.p.c.m. 8 febbraio 1999, non era dato conoscere figure di estensione della validità di un atto e, in particolare, di un contratto.

Piuttosto, in ambito contrattualistico, si conoscono figure di invalidità derivata:

così, l'art. 1419 c.c. dispone l'estensione dell'invalidità di singole clausole contrattuali all'intero regolamento negoziale, se risulta che le parti non lo

avrebbero concluso senza quella parte del suo contenuto che è colpita dalla nullità. A livello processualcivilistico è nota la figura dell'estensione dell'invalidità agli atti susseguenti collegati eziologicamente all'atto viziato (art. 159 c.p.c.); a livello amministrativo è, analogamente, conosciuta la figura dell'invalidità del provvedimento della Pubblica Amministrazione quando sia viziato l'atto presupposto.

Fatte queste precisazioni, la lettura di quanto statuito dall'art. 60 del d.p.c.m. porterebbe ad affermare che l'esistenza giuridica del documento informatico è condizionata alla "scadenza" di uno dei suoi elementi costitutivi, nella specie la sottoscrizione digitale, e che, conseguentemente, gli eventuali atti di disposizione del proprio patrimonio hanno una validità più o meno limitata nel tempo, di fatto rimessa alla discrezione delle parti contraenti. Anzi, si potrebbe affermare che il venir meno della validità di un contratto informatico a forma vincolata (art. 1350 c.c.) per la "mancanza sopravvenuta" di uno dei suoi requisiti costitutivi, nel caso di specie la firma digitale (che rispetto a questo tipo di contratti assume sicuramente il ruolo di "sottoscrizione - forma"), configurerebbe un'ipotesi, non di mera annullabilità bensì, di nullità (arg. ex. art. 1325 n. 4 c.c.) come tale dispiegante retroattivamente i suoi effetti.

Conseguenze del genere sono da considerarsi sicuramente inaccettabili sul piano della *certezza* del diritto. Occorre, quindi, interpretare il disposto dell'art. 60 cit. alla luce di quello che è il funzionamento di un sistema di firma digitale e tenendo conto del fatto che, probabilmente, la novità e

l'estremo tecnicismo della materia può aver portato, incolpevolmente, il legislatore a formulare in modo non appropriato le norme regolamentari.

Appare, opportuno, preliminarmente, fare alcune considerazioni.

Il giudizio di validità di un atto e, in particolare, di un contratto dev'essere formulato in relazione alla situazione di fatto e alle norme vigenti al *momento del suo perfezionamento*. Le vicende successive non toccano, di massima, tale giudizio.

Potrà porsi, al più, un problema di cessazione anticipata degli effetti di un contratto o della loro mancata produzione pur in presenza di un contratto valido: è il caso, quest'ultimo, della sottoposizione degli effetti di un contratto al verificarsi di una condizione sospensiva poi non avveratasi, pur essendo possibile (art. 1354 c.c.: il contratto pur essendo pienamente valido è improduttivo di effetti).

Il documento, quale "rappresentazione di un fatto giuridicamente rilevante", a mente quanto prescrive l'art. 1350 c.c., assolve ad una duplice funzione: l'atto della sua creazione, cioè l'attività di documentazione, assolve quello che è il requisito della forma (il forma-rsi del documento) richiesto dal legislatore perché si abbia la valida costituzione, modificazione ed estinzione di determinati rapporti giuridici. Ne deriva che la validità di un contratto formale è raggiunta, in presenza degli altri requisiti previsti dall'art. 1325 c.c., al momento stesso dell'esaurimento dell'attività di creazione del medesimo, che coincide con la sua perfezione; il prodotto di tale attività, lo

scritto appunto, attiene, invece, ad un profilo esclusivamente probatorio, come tale, destinato ad *estendersi* nel tempo³⁸.

Se interpretiamo l'art. 60 cit. alla luce di queste considerazioni, ne deriva che l'utilizzazione del termine "validità", da parte delle norme autorizzate, deve essere riferito all'efficacia probatoria del contratto informatico e non al giudizio sulla sua esistenza/inesistenza, che per definizione va circoscritto al momento in cui raggiunge la sua perfezione.

Quanto qui affermato trova conferma se si considera che la validità di un documento informatico è tale indipendentemente dall'apposizione di una valida firma digitale, mutando solo, rispetto ad essa, la forza probatoria che gli viene, a seconda dei casi, riconosciuta. La particolare efficacia probatoria del documento informatico sottoscritto digitalmente è, però, legata indissolubilmente alla *validità* del relativo certificato: validità che non attiene al profilo sostanziale del documento elettronico ma riguarda "l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti".

È dunque più coerente con il sistema di funzionamento complessivo della firma digitale interpretare il termine "validità" di cui all'art. 60 dell'Allegato tecnico come afferente alla validità del certificato, che a sua volta determina la "validità" sul piano probatorio del documento informatico sottoscritto con la chiave privata, sulla cui titolarità il certificato si pronuncia. D'altra parte la stessa validità/invalidità della marca temporale non incide sugli aspetti

³⁸ Cfr. GUIDI, *Teoria giuridica del documento*, Milano, 1950.

sostanziali del documento informatico cui è apposta, ma solo su quelli probatori.

Concludendo si può affermare che l'art. 60 del d.p.c.m. 8 febbraio 1999 configura, sostanzialmente, un *onere* a carico delle parti contraenti, consistente nel periodico sottoporre il documento informatico, rappresentante il loro regolamento negoziale, a validazione temporale, inadempito il quale si verifica una sorta di declassamento probatorio del medesimo, che non avrà più efficacia di prova legale, ma la meno penetrante efficacia probatoria delle riproduzioni meccaniche (arg. ex art. 5, comma 2, del D.P.R. 513). Ne deriva che il documento elettronico potrà costituire, così, principio di prova scritta ai sensi dell'art. 2724 c.c. rendendo, quindi, ammissibile la prova per testimoni⁹⁹.

⁹⁹ L'art. 2725 c.c., infatti, al secondo comma, inibisce il ricorso alla prova testimoniale quando la forma scritta, ex art. 1350 c.c., è richiesta dal legislatore sotto pena di nullità. Scaduto, però, il certificato relativo alle chiavi di sottoscrizione (o comunque revocato o sospeso) e in mancanza di valida apposizione, anteriore alla scadenza, revoca o sospensione, di una marca temporale si produrranno gli effetti di cui all'art. 10, comma 5, del D.P.R. 513: l'eventuale contenzioso fra le originarie parti contraenti, ad esempio un giudizio di accertamento circa la costituzione contrattuale di una servitù prediale, non potrà più risolversi mediante la semplice produzione del documento contrattuale informatico perché non più idoneo a valere come scrittura privata. Il documento informatico subirà una compressione della sua originaria efficacia probatoria, di guisa che non costituirà più prova legale ma, bensì, prova liberamente apprezzabile dal giudice ex art. 116 c.p.c.. Infatti, assunta la meno pregnante efficacia probatoria delle riproduzioni meccaniche, potrà valere, al più, come principio di prova per iscritto (ex art. 2724 " *qualsiasi scritto, proveniente dalla persona contro la quale è diretta la domanda o dal suo rappresentante, che faccia apparire verosimile il fatto allegato*"), non avendo ritenuto la dottrina, rispetto alla fattispecie in esame, necessaria la sottoscrizione quando sia altrimenti accertabile la provenienza della scrittura (d'altra parte un aiuto in tal senso viene dall'art. 27, comma 3, del d.p.c.m. 8 febbraio 1999 là dove dispone l'obbligo per il certificatore di conservare i certificati relativi a chiavi scadute, revocate o sospese per un periodo almeno decennale).

6. COPIE DI ATTI E DOCUMENTI IN FORMA ELETTRONICA

L'art. 6 del D.P.R. 513/97 ribadisce quella che è una caratteristica precipua del documento informatico rispetto a quello tradizionale cartaceo, e cioè il fatto che con la documentazione elettronica si verifica un completo distacco del contenuto (cioè l'elemento spirituale o intellettuale del documento: in sostanza, il pensiero materializzato nello scritto) dal contenente (cioè l'elemento materiale del documento: in sostanza, il mezzo nel quale è incorporata la scritturazione). In particolare, con riferimento al documento cartaceo, una tale scissione sarebbe inconcepibile, pena la perdita dell'efficacia sostanziale (art. 1350 c.c.) e probatoria (art. 2702 c.c.) che gli è propria: tanto l'integrità, quanto l'imputabilità fondano, infatti, la loro garanzia sul collegamento col supporto: la sottoscrizione, in quanto tale, svolge le sue funzioni solo perché legata indissolubilmente al supporto materiale. Al contrario, le garanzie fornite da un documento elettronico con firma digitale sono indipendenti da qualsiasi tipo di supporto materiale (contenente), ma si fondano solo sul modo di essere di certi contenuti. In altri termini un'autenticazione basata solo su strumenti software e non hardware¹¹⁵: ne deriva che il supporto, rispetto al documento informatico,

¹¹⁵ Così ZAGAMI, *La firma digitale*, relazione al convegno di Catania del 25 ottobre 1996 su: "Diritto, telematica e amministrazione della giustizia", all'indirizzo http://lex.unict/news/convegni/convegno_25-10/zagami/relazione.htm; vedi anche ID., *Riflessioni sul documento elettronico e sulle nuove prospettive offerte dalle firme digitali basate sulla crittografia asimmetrica*, 1996, al sito www.jei.it.

assume i caratteri della *fungibilità*²⁵, essendo possibile la sua sostituzione senza che ciò influisca sulla riproduzione del contenuto.

Il legislatore, quindi, riconoscendo, di fatto, la non-distinguibilità tra copia e originale di un documento informatico accoglie pienamente la definizione di quest'ultimo come *documento immateriale*, in virtù della sua attitudine a mantenere inalterata la propria efficacia probatoria, indipendentemente dal tipo di supporto su cui venga registrato.

Passiamo ora all'esame dell'art. 6 cit., rubricato "Copie di atti e documenti", che così dispone:

1. *I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.*
2. *I documenti informatici contenenti copia o riproduzione di 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, hanno piena efficacia, ai sensi degli artt. 2714 e 2715 c.c., se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente regolamento.*
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*

²⁵ Vedasi I. TRICOMI, *L'impronta elettronica trova la sua fisionomia: sotto controllo effetti giuridici ed efficacia*, in Guida al diritto, 4 aprile 1998, n. 13, p. 32.

all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3.

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 ai sensi dell'art. 3.

Da una lettura appena attenta dell'articolo sopra riportato, risulta evidente l'importanza dei commi primo, secondo e terzo, dedicati, rispettivamente, il primo, alle copie degli originali informatici mentre i successivi due riguardano le copie informatiche di documenti originali cartacei.

Il primo comma dell'art. 6 ha suscitato problemi interpretativi in dottrina, potendosi distinguere fra chi (Zagami)¹³³ intende circoscritta la sua portata precettiva alle sole copie informatiche del documento elettronico e chi, invece, ritiene applicabile la norma qualsiasi sia la natura, informatica o

¹³³ Sostiene Zagami, in *La firma digitale tra soggetti privati nel regolamento...*, cit., p. 925, che non disciplinando, l'art. 6 comma 1, il passaggio "dal supporto informatico al supporto non informatico (carta o altro), cioè l'effettuazione di *copie cartacee di documenti informatici* (con o senza firma digitale)" ne deriva che "affinché alla copia cartacea sia attribuito il valore probatorio dell'originale informatico, è indispensabile l'intervento del notaio o del pubblico ufficiale che attesti la conformità della copia su carta (in applicazione estensiva dell'art. 2719 c.c.)".

tradizionale-cartacea, della copia medesima (Albertini)^{4□}. A parere di chi scrive, appare preferibile la seconda delle opinioni riportate, considerato che il comma in questione non esclude in modo esplicito questa possibilità che, quindi, deve ritenersi legittimamente praticabile.

Indipendentemente da quale delle due tesi si voglia sposare, dal 1 comma dell'art. 6 discende che ogni duplicato, copia e estratto *informatico* di un documento elettronico, anche se trasmesso telematicamente, conserva la stessa efficacia probatoria dell'originale, senza che occorra l'intervento del notaio o altro pubblico ufficiale a garanzia dell'integrità del contenuto.

Pertanto, relativamente al *tipo* di efficacia probatoria propria delle copie di cui all'art. 6 comma 1, in aderenza alla tesi prima sostenuta, bisognerà distinguere: se trattasi di copia informatica di documento elettronico, in applicazione del principio di immaterialità del documento informatico, *nulla quaestio*; se trattasi, invece, di copia cartacea, dovrà dirsi inoperante il principio di cui sopra (siamo, infatti, in presenza di un documento informatico in senso ampio) e quindi propendersi per l'applicabilità analogica dell'art. 2719 c.c.: occorrerà cioè l'attestazione di conformità del pubblico ufficiale o, in mancanza, il non disconoscimento della parte contro cui viene prodotta la copia^{5□}.

^{4□} ALBERTINI, *Sul documento informatico e sulla firma digitale*, cit., p. 280 e nota n. 41.

^{5□} ALBERTINI, *op. cit.*, p. 281, ritiene, invece, estensibile il dispositivo di cui all'art. 2719 c.c. anche alla copia informatica di originale elettronico.

Per quanto riguarda, invece, la questione relativa al *quantum* di efficacia probatoria delle copie, questa sarà strettamente correlata a quella propria dell'“originale” informatico: così, la copia di un documento sottoscritto digitalmente avrà l'efficacia probatoria di cui all'art. 2702 c.c.; se l'originale non era firmato digitalmente, la copia avrà il valore probatorio delle riproduzioni meccaniche; se trattasi di copia di un documento informatico autenticato ex art. 16 D.P.R. 513, la copia ha il valore di una scrittura privata autenticata ex art. 2703 (*rectius*: la maggiore efficacia probatoria prevista dallo stesso art. 16 che, come vedremo, rappresenta un *quid pluris* rispetto alla tradizionale autenticazione: ne deriva una compressione dell'oggetto della querela di falso); la copia della copia informatica di un atto pubblico cartaceo (ex art. 6, comma 2, del D.P.R.) avrà l'efficacia probatoria dell'atto pubblico ex art. 2700 c.c.

Alla luce di quanto esposto, pare scelta “anacronistica” quella compiuta dal legislatore riguardo la distinguibilità tra *originale* e *copia*⁶³, propria del cartaceo, riferita ai documenti informatici. Infatti, come sottolineato dalla dottrina “in realtà, la stessa nozione di originale, e quella collegata di copia, perdono significato, se solo si pone mente alla circostanza che i documenti informatici sono tutti originali, non distinguendosi in nulla la copia dal

⁶³ Il primo comma dell'art. 6 menziona anche l'estratto del documento informatico, il quale sarà soggetto alla disciplina di cui all'art. 2718 c.c., farà cioè piena prova solo per quella parte del documento informatico originale che riproduce letteralmente.

documento originariamente creato; più correttamente si parlerà, allora, di duplicati”⁷⁷⁸.

Quanto affermato, risulta dalla considerazione che si ha *copia* quando il fatto rappresentato è il documento medesimo (ne deriva che le copie possono definirsi “documenti di secondo grado”⁹ perché non rappresentano direttamente l’atto, ma lo fanno indirettamente attraverso la rappresentazione del documento che lo contiene), mentre si ha l’*originale* quando la rappresentazione dell’atto è diretta: ne deriva che non può tecnicamente definirsi copia un’evidenza informatica perché essa offre esattamente la stessa rappresentazione del *file* di partenza.

I successivi commi secondo e terzo si riferiscono entrambi alle copie su supporto informatico di originali cartacei.

In realtà, la lettura del terzo comma dell’articolo in esame può portare all’obiezione che solo quest’ultimo si riferisca alla copia di originali cartacei, mancando al comma precedente l’indicazione esplicita ai “documenti formati *in origine* su supporto cartaceo”. L’obiezione, però, è subito superata se si considera che, così opinando, dovrebbe risultare pleonastico e del tutto fuor

⁷⁷ M. MINERVA, *L’attività amministrativa in forma elettronica*, in Foro Amm., 1997, p. 1311; così anche ORLANDI, *La paternità delle scritture*, cit., p. 502 secondo il quale “l’antitesi tra copia e originale si restringe ad un *piano puramente cronologico*, poiché i documenti hanno per definizione la medesima sostanza informatica...Dinanzi a due dischi, recanti il medesimo contenuto informatico, poco importa stabilire quale sia l’originale o quale la copia: essi restituiscono la medesima informazione elettronica”.

⁷⁸ Per “duplicato” deve intendersi un’ulteriore documentazione, sorta simultaneamente all’originale, della medesima dichiarazione. Così IRTI, *La riproduzione del negozio giuridico*, Milano, 1970, p.120; per la definizione di copia, estratto, duplicato certificato ecc. vedi M. DI FABIO, *Manuale di notariato*, Milano, 1981, p.195.

⁷⁹ CARNELUTTI, *La prova civile*, cit., p. 215.

di luogo, quando trattasi di una scrittura privata informatica autenticata e depositata presso il notaio¹⁰, il richiamo, fatto dall'art. 6 comma 2, alla necessità dell'apposizione della firma digitale di quest'ultimo, onde garantire alla copia la stessa efficacia dell'originale, dato che l'autentica di una scrittura privata informatica richiede già, ex art.16 comma 3 D.P.R. 513, l'apposizione della firma digitale dell'ufficiale autenticante.

La differenza, di carattere precettivo, tra quanto dispongono il secondo e il terzo comma, pur riferendosi entrambi alla copia informatica di documenti in origine cartacei, è stata individuata¹¹ nella diversa qualificazione attribuita a questi ultimi. Così, il riferimento fatto dal *secondo comma* dell'art. 6 ai documenti di cui agli artt. 2714-5 c.c. va riferito alle copie di atti pubblici o di scritture private o comunque di *documenti depositati* in originale presso pubblici ufficiali o pubblici depositari autorizzati¹².

¹⁰ Come, infatti dispone l'art. 72, ultimo comma, della L. 16 febbraio 1913, n. 89 (legge notarile) "le scritture private autenticate dal notaio, verranno, salvo contrario desiderio delle parti restituite alle medesime".

¹¹ ALBERTINI, *Sul documento informatico e sulla firma digitale*, cit., p.282-3; vedi anche F. DE SANTIS, *op. cit.*, p. 390-91.

¹² Il legislatore non individua i soggetti che vanno considerati pubblici depositari. La Cassazione ha ritenuto che la norma non faccia riferimento ai pubblici funzionari i quali abbiano a disposizione gli atti dell'ente pubblico per motivo del loro ufficio, ma solo quelli che hanno la *specifica funzione di conservare* e tenere a disposizione del pubblico gli atti che hanno rogato, contribuito a formare o ricevuto in deposito: notai, conservatori dei Registri Immobiliari e cancellieri. Così Cass, 3 marzo 1961, n. 456, in *Giust. Civ.*, 1961, I, p. 999. Ne deriva che sarà regolata dal comma secondo dell'articolo in esame, anziché dal successivo, la copia informatica di scrittura privata autenticata, del cui originale le parti abbiano chiesto il deposito presso il notaio, come previsto dall'art. 72, ultimo comma, l. notarile. Al contrario, nel caso in cui le parti abbiano consegnato al notaio la scrittura privata autenticata a titolo di deposito meramente fiduciario, come potrebbero fare con qualsiasi persona di fiducia, opererà il comma terzo dell'art. 6: infatti, la figura del notaio non rileverà più, in tale ipotesi, come pubblico ufficiale.

Al contrario, la disciplina prescritta al *terzo comma* va riferita alle copie di *documenti* originali cartacei *non depositati* presso pubblici ufficiali o pubblici depositari autorizzati.

Ne deriva che, nel primo caso, i documenti informatici contenenti copia di originali cartacei depositati presso pubblici ufficiali acquistano l'efficacia probatoria dell'originale se ad essi è apposta od associata la firma digitale del pubblico depositario autorizzato o del pubblico ufficiale.

A ciò si aggiunga che ex art. 6 comma 4 del D.P.R. 513 “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”.

Il terzo comma, invece, non richiede l'apposizione della firma digitale del notaio o del pubblico depositario autorizzato al fine di determinare la piena fungibilità tra originale cartaceo e copia informatica. Questo perché trattasi di documenti originali cartacei non depositati pubblicamente o depositati presso un pubblico ufficiale a titolo fiduciario (di modo che non sorge lo specifico dovere pubblico di conservare un atto o documento, essendo tale attività sussumibile entro gli schemi dell'autonomia privata). Si richiede, invece, un'attestazione (è termine preferibile rispetto ad “autenticazione”, essendo la disciplina ricalcata su quella dell'art. 2719 c.c.) di conformità all'originale con dichiarazione allegata al documento informatico e rispondente alle specifiche tecniche di cui al d.p.c.m. 8 febbraio 1999. Un *quid minus*, quindi, rispetto alla firma digitale dal punto di vista delle formalità richieste al

pubblico ufficiale ma mantenendo inalterata, rispetto al comma precedente, la garanzia circa la conformità all'originale cartaceo.

Questa costruzione interpretativa, sebbene abbia il pregio di mantenere distinti, a livello precettivo, i commi 2 e 3 dell'articolo 6 del D.P.R. 513 (che sicuramente non brillano per chiarezza espositiva), tuttavia non convince.

Rimane, infatti, un dato ineluttabile: che anche a volere mantenere distinta la disciplina relativa all'attestazione di conformità della copia informatica in relazione alla diversa *qualità* dell'originale cartaceo, rimane comunque il fatto che, l'"autenticazione di conformità" di cui al comma 3 dell'art. 6 se, a livello descrittivo, può evocare un *quid minus* rispetto alla firma digitale del pubblico ufficiale richiesta dal comma precedente, non può, di fatto, risolversi in qualcosa di diverso da quest'ultima: il notaio, infatti, non ha altro mezzo di imputazione di cui avvalersi per garantire la riferibilità alla sua persona dell'attestazione informatica di conformità, da lui effettuata, della copia elettronica all'originale cartaceo¹³.

¹³ D'altra parte, lo stesso F. DE SANTIS, *op. cit.*, p. 391 nota n. 36, si vede costretto ad ammettere il ricorso allo strumento della firma digitale per autenticare la conformità delle copie informatiche agli originali di cui al comma 3 dell'art. 6 del D.P.R. 513, e ciò in base al raffronto con quanto dispone l'art. 16 comma 3 del regolamento governativo. Non appare poi condivisibile la tesi, avanzata dallo stesso A., secondo cui l'utilizzo del termine "allegata", fatto dal legislatore al comma 3 dell'art. 6, tenuto conto della definizione che la dottrina usualmente fornisce del termine "allegato" in relazione alla legge notarile (art. 51 L. not.: CASU, *L'atto notarile tra forma e sostanza*, Milano-Roma, 1996, p. 208), tradizionalmente considerato come documento cartaceo, legittimerebbe la possibilità per il notaio di rilasciare una dichiarazione scritta su supporto cartaceo, il cui contenuto faccia riferimento circostanziato ad un supporto informatico su cui è incisa la copia. A tale conclusione ostano sia motivi di ordine pratico che normativo. Infatti, non avrebbe senso riconoscere la piena fungibilità tra copia informatica e documento originale cartaceo quando la maggiore velocità di circolazione della prima dovesse risultare compromessa dalla necessità di dover esibire un'attestazione di conformità su carta; a ciò si aggiunga che le modalità di allegazione al documento elettronico di altri documenti formati su supporto diverso da quello informatico trova già una sua disciplina, e precisamente al comma 4 dell'art. 16 del D.P.R. 513, che così dispone: "Se al documento informatico...deve essere

Appare, allora, preferibile la tesi di chi¹⁴ interpreta i commi secondo, terzo e quarto come riferibili agli originali cartacei *tout court*, senza distinzione relativa al fatto che siano o meno depositati presso notai o pubblici depositari autorizzati, essendo analoga, di fatto, la procedura da seguire per attestare la conformità delle copie informatiche agli originali. Ne consegue che i commi summenzionati debbono essere letti come un'unica previsione di *copie informatiche autenticate di documenti cartacei* (*rectius*: documenti comunque non-digitali) le quali “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” (art. 6 comma 3 et art. 16 comma 4).

Tale autentica consiste nella dichiarazione di conformità resa dal pubblico ufficiale allegata (art. 16 comma 4 D.P.R. 513) alla copia informatica dell'originale cartaceo. L'attestazione di conformità di cui sopra necessiterà dell'apposizione o associazione della firma digitale del pubblico ufficiale analogamente a quanto è previsto dal secondo comma dell'art. 6, il quale attribuisce l'efficacia probatoria della scrittura privata o dell'atto pubblico originale, alle copie informatiche spedite o rilasciate ai sensi degli artt. 2714 e 2715 c.c. “se ad esse è apposta o associata la firma digitale del pubblico ufficiale che le rilascia”.

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'art. 6 del presente regolamento”.

L'art. 6 del D.P.R. 513 al comma 4, è norma di ampia portata, poiché, disponendo l'esonero dalla esibizione e produzione degli originali cartacei (se richiesti da specifiche norme di legge) quando siasi in possesso di copie informatiche autenticate, rende possibile, ad esempio, iscriversi telematicamente al registro delle imprese anche quando l'atto da iscrivere sia una scrittura privata autenticata non depositata presso notaio (dovendosi ritenere, per effetto del D.P.R. 513, abrogato implicitamente il disposto dell'art. 11, comma 4, del D.P.R. 581/95) e assolvere, sempre telematicamente, gli adempimenti richiesti dall'art. 2658 c.c. per la trascrizione nei registri immobiliari¹⁵.

Come sottolineato da Rognetta¹⁶ la norma sopra riportata rappresenta “un ulteriore passo avanti sulla strada della liberazione dagli *intralci* cartacei: infatti, quando la legge richiede la produzione di un originale cartaceo, il cittadino potrà, in sua vece, produrre la copia autentica digitale. La differenza più rilevante è che non si sarà più costretti a portare con sé l'originale cartaceo per consegnarlo al proprio interlocutore, ma sarà sufficiente una produzione telematica della copia informatica debitamente autenticata, che

¹⁴ Vedi in proposito ROGNETTA, *La firma digitale e il documento informatico*, cit., p. 75-8 e ZAGAMI, *La firma digitale tra soggetti privati...*, cit., p. 924.

¹⁵ La contraria tesi di PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, cit., p. 587 non risulta accoglibile perché viziata *ab origine* dalla erroneo inquadramento del D.P.R. 513 fra i regolamenti di attuazione quando, invece, per espresso richiamo della legge autorizzatrice, esso va inquadrato nella categoria dei regolamenti di delegificazione (art. 17, comma 2, L. 400/88) che, come tali, sono capaci di modificare disposizioni sovraregolamentari aventi la qualifica di legge ordinaria.

¹⁶ ROGNETTA, *La firma digitale e il documento informatico*, cit., p. 78.

potrà viaggiare, senza necessità di alcun accompagnatore, sulle reti telematiche, al fine di raggiungere il suo destinatario”.

Sulla stessa scia, si colloca, infine, il comma 5 dell’art. 6 che pone una norma generale secondo cui tutti gli obblighi di “conservazione e di esibizione” di documenti possono venire soddisfatti mediante documento informatico. La norma assume notevole importanza poiché, per un verso, dovunque una norma di legge prescriva la conservazione di documenti può ritenersi bastevole la sola memorizzazione digitale con facoltà di distruzione del cartaceo e, per altro verso, l’esibizione in processo potrà avvenire tramite copia informatica.

7. LIBRI SCRITTURE CONTABILI

La disciplina codicistica sulla tenuta obbligatoria delle scritture contabili ha la funzione di preconstituire uno strumento di controllo sull'attività degli imprenditori commerciali (non piccoli, ex art. 2214 ultimo comma c.c.), nell'interesse di quanti entrano con essi in rapporto ed acquistano, nei loro confronti, ragioni di credito¹.

Le scritture contabili che l'imprenditore deve tenere sono il libro giornale e il libro degli inventari (a cui devono essere aggiunte le altre scritture contabili che siano richieste dalla natura e dalle dimensioni dell'impresa).

Le scritture contabili sono sottoposte ad un regime di formalità estrinseche ed intrinseche a garanzia, data la funzione di documentazione svolta dalle stesse, della loro inalterabilità e corretta compilazione. Le scritture contabili sono regolari, sotto il primo aspetto, se sono state osservate le prescrizioni di cui agli artt. 2215, 2216, 2217 comma 3: in particolare, ex art. 2215, il libro giornale e il libro degli inventari sono regolari, dal punto di vista intrinseco, se regolarmente bollati e numerati progressivamente in ogni pagina, prima del loro utilizzo, dall'ufficio del registro delle imprese o da un notaio.

Quanto al secondo aspetto, le scritture contabili, sono considerate regolari dal punto di vista estrinseco se "tenute secondo le norme di un ordinata contabilità" (art. 2219 c.c.).

¹ Sull'argomento vedasi PANUCCIO, *Natura giuridica delle registrazioni contabili*, Napoli, 1964.

Gli interessi protetti dalle norme summenzionate sono quelli di singoli creditori, che dalle scritture contabili possono trarre la prova delle proprie pretese verso l'imprenditore. È, infatti, stabilito, che "i libri e le altre scritture contabili delle imprese soggette a registrazione fanno prova contro l'imprenditore" (art. 2709 c.c.): si produce quindi un'inversione dell'onere della prova, in base al quale chi vanta un credito nei confronti dell'imprenditore non dovrà accollarsi l'onere di dimostrare le proprie pretese, conformemente a quanto disposto dall'art. 2697 c.c., essendogli sufficiente chiedere l'esibizione delle scritture contabili del suo debitore, dalle quali *deve* risultare la registrazione del corrispondente debito. Tuttavia, proprio perché le scritture contabili attengono a un profilo squisitamente probatorio e non costitutivo dei diritti, da cui derivano le pretese fatte valere in giudizio dal creditore, all'imprenditore è data sempre facoltà di fornire la prova contraria. La regolare tenuta delle scritture contabili è inoltre idonea a far sì che esse costituiscano prova a favore dell'imprenditore, ma solamente quando la controparte sia altro soggetto a cui sia obbligatoriamente imposta la tenuta delle medesime (art. 2710 c.c.). È bene precisare che per aversi prova contro l'imprenditore non è necessario che le scritture siano regolarmente tenute come non è necessario che si tratti di "libri bollati e numerati nelle forme di legge", configurando queste prescrizioni un onere a carico dell'imprenditore solo per l'ultima delle fattispecie esaminate:

comunque, tanto nell'uno quanto nell'altro caso, si tratta di prove la cui valutazione è rimessa al libero apprezzamento del giudice²².

L'obbligo della tenuta delle scritture contabili è poi strettamente connesso all'obbligo della loro conservazione: è infatti disposto che devono essere conservate da parte dell'imprenditore per dieci anni dalla data dell'ultima registrazione, unitamente agli originali delle lettere, telegrammi e fatture spedite oltre che le copie delle lettere, telegrammi e fatture spedite (art. 2220 c.c.). La norma assume rilievo, non tanto per le conseguenze immediate della sua violazione, quanto per la rilevanza penale in caso di fallimento dell'obbligato: l'art. 217, comma 2, del R.D. 16 marzo 1942, n. 267 dispone, infatti, che l'imprenditore dichiarato fallito, che risulti non avere tenuto le scritture contabili nei tre anni anteriori al fallimento o che risulti averle tenute irregolarmente, è punito per il reato di bancarotta semplice²³; il precedente art. 216, al n. 2, prescrive, invece, il reato di bancarotta fraudolenta per l'imprenditore dichiarato fallito, che risulti avere distrutto o falsificato, per procurare a sé o ad altri un ingiusto profitto o per recare pregiudizio ai creditori, le scritture contabili o che risulti averle tenute in modo da non rendere possibile la ricostruzione del suo patrimonio o del movimento dei suoi affari.

²² Così Cass., 9 aprile 1987, n. 3499, in *Mass. Foro it.*, 1987.

²³ È vero che l'articolo appena citato parla di responsabilità penale derivante da mancata o irregolare tenuta delle registrazioni contabili ma corrisponde anche a verità che, come è stato ben puntualizzato, l'obbligo di *conservare* è una conseguenza logica dell'obbligo di *tenere* le scritture contabili, sicché la distruzione anteriore al decennio equivale a mancata tenuta. Così BOCCHINI, *Manuale di diritto della contabilità delle imprese*, I, Torino, 1989; cfr. anche C. PASTERIS, *Diritto commerciale*, in *Noviss. Dig. it.*, V, Torino, 1960.

Compiuta questa breve disamina introduttiva, è dato notare come l'ingresso della documentazione informatica nel settore relativo alla tenuta e conservazione delle scritture contabili, antecedentemente all'emanazione del D.P.R. 513, sia stato residuale, ammettendosi, a partire dal 1994, la conservazione delle scritture su supporti di immagini ma non la loro tenuta informatica, potendo essere quest'ultima solo provvisoria e dandosi, comunque, per presupposta l'esistenza di registri cartacei previdimati. Così, con il D.L. 10 giugno 1994 n. 357, poi convertito in legge, con modificazioni, dall'art. 1 della L. 489/94 (recante "Disposizioni tributarie urgenti per accelerare la ripresa dell'economia e dell'occupazione, nonché per ridurre gli adempimenti a carico del contribuente"), si dispose:

— all'art. 7-*bis* comma 3, introduttivo di un nuovo ultimo comma all'art. 2220 c.c., che "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".

— all'art. 7 comma 4-*ter*, che "A tutti gli effetti di legge , la tenuta di qualsiasi registro contabile con sistemi meccanografici è considerato regolare in difetto di trascrizione su supporti cartacei, dei dati relativi all'esercizio corrente, allorché quando anche in sede di controlli ed ispezioni gli stessi risultino aggiornati sugli appositi supporti magnetici e vengano stampati

contestualmente alla richiesta avanzata dagli organi competenti ed in loro presenza”. La norma non consente quindi *tout court* la tenuta della contabilità sotto forma di documento informatico in senso stretto; solo consente, in caso di mancata trascrizione su carta, nei termini di legge, dei dati contabili relativi all’esercizio in corso, la loro provvisoria memorizzazione digitale, a fini di aggiornamento, mediante l’ausilio di un elaboratore in grado, comunque, di fissare le operazioni su carta.

Ebbene, il quadro fin qui descritto risulta totalmente modificato dal regolamento sulla firma digitale che consente ora non solo di conservare in forma digitalizzata i dati contabili delle imprese ma anche, e sempre in forma digitale, il soddisfacimento dei requisiti relativi alla loro tenuta.

La normativa di riferimento deve essere individuata, principalmente, nell’art. 15 del D.P.R. 513, rubricato “Libri e scritture”, ma vengono in rilievo anche il secondo comma dell’art. 5, dedicato all’efficacia probatoria del documento informatico, nonché l’ultimo comma dell’art. 6 relativo alle copie.

Il primo di questi articoli dispone che i libri, i repertori e le scritture, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici a condizione che ciò avvenga nel rispetto del regolamento e delle regole tecniche di cui al d.p.c.m. 8 febbraio 1999. L’art. 6, relativo alle copie informatiche, stabilisce la soddisfazione degli obblighi di conservazione, previsti dalle vigenti disposizioni legislative, anche se la documentazione assume la forma elettronica, purché quest’ultima sia conforme alle disposizioni regolamentari. L’art. 5 comma 2, afferma che il documento

informatico sfornito di firma digitale “soddisfa l’obbligo previsto dagli artt. 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa e regolamentare”.

In base a queste norme diventa ora possibile non solo la conservazione ma anche la tenuta su supporto informatico delle scritture contabili, dovendosi considerare abrogate tutte le disposizioni di legge con esse incompatibili.

Ci si potrebbe chiedere se la novella abbia abrogato, in forza dell’art. 5 comma 2, anche le disposizioni relative alle modalità estrinseche ed intrinseche di tenuta delle scritture, dato che abbiamo visto essere subordinata l’efficacia probatoria, a favore dell’imprenditore, di queste ultime alla loro preventiva numerazione e vidimazione³⁴.

Pare doversi propendere per la soluzione positiva al quesito, dato l’esplicito tenore dell’art. 5 che parla di soddisfazione “dell’obbligo previsto dagli articoli 2214 e *seguenti*”. Tra l’altro, già antecedentemente all’emanazione del regolamento sulla firma digitale la giurisprudenza si era espressa per la sufficienza del rispetto delle sole formalità intrinseche.³⁵

L’art. 15 del regolamento, unitamente alle altre norme richiamate, non si limita, però, a stabilire l’equiparabilità ad ogni effetto di legge tra la tenuta informatica e quella cartacea con esclusivo riferimento alle registrazioni

³⁴ La regolare tenuta e vidimazione dei libri contabili è posta come condizione della loro efficacia probatoria da Cass., 23 ottobre 1976, in Foro it., Rep. 1976, voce *Libri e scritture contabili*, n. 3.

³⁵ Cfr. DE SANTIS, *Op. cit.*, p. 396 e *ivi* per i riferimenti giurisprudenziali.

contabili, ma estende la sua portata precettiva a qualsiasi altro libro o scrittura di cui sia obbligatoria la tenuta.

Ne consegue che, in base ad esso, le società di capitali, le imprese cooperative e le mutue assicuratrici potranno avvalersi della forma elettronica per la tenuta del libro dei soci (art. 2421 c.c.), del libro delle obbligazioni (art. 2490 c.c.) e del libro delle adunanze e delle deliberazioni degli obbligazionisti (art. 2516 c.c.: questi ultimi soltanto per le s.p.a. e per le s.a.p.a., la cui disciplina si modella ex art. 2464 c.c. su quella delle s.p.a.), del libro delle adunanze e delle deliberazioni delle assemblee, del consiglio di amministrazione e dell'eventuale comitato esecutivo (solo per le s.p.a. e per le s.a.p.a.), del libro delle adunanze e deliberazioni del collegio sindacale (possibilità che deve riconoscersi anche per le s.r.l. che abbiano un capitale sociale superiore a duecento milioni o se la nomina del collegio è stabilita nell'atto costitutivo ovvero se per due esercizi consecutivi vengono superati due dei limiti di cui all'art. 2435 *bis* c.c. primo comma).

Parimenti, in base all'art. 15 cit. le società di capitali, le imprese cooperative e le mutue assicuratrici potranno avvalersi della forma elettronica per la redazione del bilancio (artt. 2423-2435 *bis* c.c.).

8. **IL KEY ESCROW FACOLTATIVO**

L'art. 7 del D.P.R. 513/97 disciplina il deposito facoltativo della chiave privata presso un notaio o altro pubblico depositario autorizzato.

Questa norma, letta in relazione all'art. 9 lett. g) del D.P.R., che pone a carico delle società di certificazione l'obbligo di non rendersi depositarie di chiavi private, denuncia una precisa scelta *politica* del legislatore italiano, orientata verso il pieno riconoscimento della legittimità dell'uso della crittografia a scopo di segretezza: nessuno, quindi, può essere costretto a depositare la propria chiave privata presso una pubblica autorità, ma, al contrario, l'eventuale deposito della chiave sarà il frutto di una libera decisione dell'utente del sistema di firma digitale.

L'importanza delle norme citate si spiega considerando che accanto ad un utilizzo lecito dei sistemi di crittografia può affiancarsi, altresì, un utilizzo criminale dei medesimi.

Se, infatti, la caratteristica peculiare di un sistema di firma digitale è quella di riuscire a garantire l'assoluta riservatezza del contenuto di un documento informatico, di modo che questo diventi intellegibile solamente al suo destinatario tramite l'apposita procedura di decifratura (attuabile con la chiave privata corrispondente a quella pubblica utilizzata per cifrarlo), ne deriva che la legittimazione incondizionata e senza restrizioni al suo utilizzo può offrire la possibilità alle organizzazioni terroristiche, come anche alla

criminalità comune, di disporre di un canale privilegiato di trasmissione delle informazioni al riparo da qualsiasi ingerenza delle autorità investigative.

Si pone quindi il problema di tutelare il diritto alla riservatezza delle comunicazioni telematiche (costituzionalmente garantito, in Italia, dall'art. 15 Cost.), senza con questo impedire attività tendenti alla repressione della criminalità

A tal uopo, prendendo come termine di paragone la legislazione sovranazionale, tradizionalmente si è fatto ricorso, alternativamente o cumulativamente, all'adozione di normative disciplinanti in modo molto restrittivo l'esportazione di sistemi crittografici “*forti*”¹ e all'imposizione di sistemi di *key escrow* o di *key recovery*.

Norme restrittive in materia di esportazione di sistemi crittografici sono rinvenibili, ad esempio, nel *Trattato di Wassenaar* del luglio 1996, regolante l'esportazione delle armi convenzionali e dei beni e delle “tecnologie a doppio uso”, cioè di quelle tecnologie utilizzabili tanto in ambito militare che civile e di cui la crittografia fa parte.

I paesi firmatari del trattato², poi rivisto con gli accordi di Vienna del dicembre 1998, tra cui l'Italia, si sono obbligati a stabilire precise restrizioni all'esportazione di crittografia oltre i 56 *bit*³.

¹ Per crittografia *forte* s'intende quella basata su algoritmi di una certa robustezza, variamente quantificata a seconda delle interpretazioni datene dalle varie autorità disciplinanti la materia nei vari paesi.

² Gli Stati aderenti, attualmente, al trattato, oltre l'Italia, sono: Argentina, Australia, Austria, Belgio, Bulgaria, Canada, Repubblica Ceca, Danimarca, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Giappone, Lussemburgo, Olanda, Nuova Zelanda, Norvegia, Polonia,

A livello di normazione interna, invece, operano i sistemi di *key escrow* e *key recovery* che si configurano, rispettivamente, come obbligo a carico dell'utente di un sistema di firma digitale e come potere della Pubblica Autorità

Precisamente, con il *key escrow* il cittadino, che voglia utilizzare un sistema di firma digitale, è previamente tenuto a depositare copia della sua chiave privata presso un ente governativo, di guisa che, se necessario, si possa ottenere la decifratura dei messaggi a lui indirizzati^{34a}.

Con il *key recovery*, invece, all'utilizzatore di un sistema di firma elettronica non viene imposto alcun deposito coattivo della chiave privata, ma la garanzia circa la riservatezza delle sue comunicazioni è, comunque, compromessa dal possesso da parte della Pubblica Autorità di una sorta di

Portogallo, Repubblica di Corea, Romania, Federazione Russa, Repubblica Slovacca, Spagna, Svezia, Svizzera, Turchia, Regno Unito, Stati Uniti, Ucraina.

^{33a} Altro esempio di normativa fortemente restrittiva in materia di esportazione dei software crittografici è data dalla legislazione statunitense. Ad esempio, l'*Office of Defense Trade Control* statunitense di norma colloca gli algoritmi superiori a 40 *bit* in questa categoria, facendo scattare, quindi, il divieto di esportazione. Cfr. ROGNETTA, *La firma digitale e il documento informatico*, op. cit., p. 21.

^{34a} Esempio, a questo proposito, era la normativa francese antecedente al 1999. Le leggi n. 1170 del 1990 e n. 659 del 1996 prevedevano, infatti, forti limitazioni all'esportazione di *software* crittografico (la cui robustezza non poteva superare la soglia dei 40 *bit*) e imponevano una preventiva autorizzazione del Primo Ministro, cui si aggiungeva la previsione di un sistema di *key escrow*. Recentemente, però, la situazione sembra votata al cambiamento: già nel gennaio del 1999 gli organi di governo francesi preso atto dell'inadeguatezza della legislazione del 1996 poiché "essa limita fortemente l'uso della crittografia (...) senza d'altronde permettere ai poteri pubblici di lottare efficacemente contro i messaggi delle organizzazioni criminali la cui cifratura potrebbe facilitare la dissimulazione" (le parole sono quelle del Primo Ministro francese Jospin, pronunciate il 19 gennaio 1999, in occasione della conferenza innanzi al Comitato interministeriale per la società dell'informazione) hanno innalzato la soglia della crittologia liberamente utilizzabile portandola da 40 *bit* a 128 *bit*, impegnandosi, tra l'altro, a sopprimere il carattere obbligatorio del ricorso al terzo di fiducia per il deposito delle chiavi di cifratura. Attualmente è stata avviata una pubblica consultazione telematica volta a delineare le linee guida di quella che sarà la futura normativa francese sulla firma digitale. Per maggiori informazioni consulta i siti <http://www.interlex.it> e <http://www.jei.it>.

“codice di sblocco” del sistema: in sostanza un “*passe – partout*” che consente di decifrare qualsiasi documento che sia stato in precedenza cifrato⁵.

Di tutto ciò non è dato trovare traccia alcuna nella normativa italiana sulla firma digitale orientata, com'è, a privilegiare, primariamente, la privacy del singolo utilizzatore del sistema piuttosto che obbedire a logiche proprie di una Stato di Polizia.

D'altra parte, non può sottacersi il fatto che la prima bozza dell'A.I.P.A. del settembre del 1996⁶ incontrò pesanti critiche da parte della comunità telematica, proprio per la previsione, ivi contenuta, di un sistema di certificazione reputato potenzialmente lesivo del diritto alla segretezza della corrispondenza telematica⁷.

Infatti, pur non adottando esplicitamente un sistema di *key escrow*, si prevedeva l'istituzione di un Consiglio Superiore delle Autorità di Certificazione (art. 12) da cui dipendevano l'Autorità Amministrativa di Certificazione, per il settore pubblico, e l'Autorità Notarile di certificazione per

⁵ Questo sistema è stato adottato, ad esempio, dal governo statunitense. Si è, infatti, istituito un apposito organismo tecnico presso l'FBI con il compito di decifrare le informazioni di presunta matrice criminosa. Al contempo, l'amministrazione statunitense, preso atto che l'adozione di una politica disincentivante l'uso della crittografia avrebbe prodotto una compressione degli investimenti e degli scambi commerciali, ha stabilito l'innalzamento della soglia massima per l'esportazione di software crittografico asimmetrico (che ora si attesta sui 1024 bit) subordinando, però, tale facoltà al rilascio di un provvedimento a carattere autorizzatorio. Cfr. A. MONTI, *Crittografia: nuove regole o regole nuove?*, in “PC Professionale”, novembre 1998.

⁶ Il testo integrale della bozza è consultabile su Internet all'indirizzo <http://idea.sec.dsi.unimi.it/SECURITY-DOC/LAW/ridotto.html>.

⁷ Gli interventi, i contributi e le critiche a questo primo progetto sono consultabili all'indirizzo <http://www.interlex.com/docdigit/indice.htm>. Vedi anche M. CAMMARATA, *Troppo burocrazia per il documento digitale*, in “MCmicrocomputer”, 1997, n.169, p.168; ID., *Key escrow, una questione molto delicata*, in “MCmicrocomputer”, 1996, n. 168.

il settore privato. Le Autorità di Certificazione potevano, a loro volta, delegare le proprie competenze, rispettivamente, ad Autorità Intermedie di Certificazione (art. 16) e ad Autorità Private di Certificazione (art. 20). Non era previsto il divieto per le Autorità di Certificazione di rendersi depositarie delle chiavi private dei propri utenti e si prevedeva l'istituzione di un archivio di chiavi, private e pubbliche, di competenza delle autorità sopra citate (art. 27). Il futuro quadro normativo si palesava, insomma, non molto diverso, nella sostanza, da quello caratterizzante le realtà oltre confine.

Il progetto, com'è noto, non si tradusse in realtà e successivamente l'A.I.P.A., recependo anche i contributi e le critiche formulate dalla comunità di Internet, ebbe modo di compilare un'altra bozza, questa volta in attuazione della delega contenuta nell'art. 15 della L. 59/97, che dopo modifiche di poco conto, superato tutto l'iter procedimentale proprio dei regolamenti di cui all'art. 17 della L. 400/88, si tradusse nel D.P.R. 513. Scomparvero, così, sia la previsione di una strutturazione gerarchica delle Autorità di Certificazione che la previsione di un archivio di chiavi, pubbliche e private, di competenza delle Autorità stesse, in favore di un sistema di firma digitale votato al rispetto del principio della riservatezza nelle comunicazioni telematiche.

Il sistema italiano, dunque, non prevede alcun deposito coattivo della chiave privata del titolare della firma digitale ma ammette la facoltatività del deposito stesso: il pubblico depositario che riceve la chiave privata non ha alcuna possibilità di utilizzarla, né per decifrare i messaggi del titolare, né per

altri motivi (arg. ex art. 7, comma 2, DPR): quindi tale deposito non inficia minimamente la tutela della riservatezza del depositante.

Ma veniamo ad un'analisi più dettagliata del disposto dell'art. 7 in esame.

Il primo comma, come accennato, prevede la facoltà di deposito, da parte del titolare di una coppia di chiavi asimmetriche, della propria chiave privata⁸ presso un notaio o altro pubblico depositario autorizzato. La chiave privata, a mente il secondo comma dell'art. 7, può essere “registrata su qualsiasi tipo di supporto idoneo a cura del depositante e dev'essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni”. Segue l'ultimo comma dell'articolo in esame, che opera un rinvio a quanto disposto dall'art. 605 c.c., relativo alle modalità del testamento segreto, in quanto applicabile.

La *ratio* della norma va individuata, principalmente, nell'esigenza che ha il privato di cautelarsi contro i rischi derivanti dalla perdita della chiave privata⁹ (ad esempio per lo smarrimento della *password* di abilitazione all'uso della chiave stessa o per la cancellazione del supporto su cui è conservata: il che lo renderebbe impossibilitato a decifrare i messaggi o le proposte contrattuali telematiche preventivamente cifrate dalla controparte

⁸ Ovviamente si tratterà di “copia” della chiave privata del titolare, dovendo quest'ultima rimanere nella disponibilità del privato per l'utilizzo quotidiano.

⁹ Ma non anche contro i rischi derivanti dalla perdita o sottrazione della chiave privata cui segua un utilizzo illegittimo della medesima da parte di terzi non autorizzati. Infatti, al di là della limitata pubblicità di fatto prevista dall'art. 10, comma 5, del D.P.R., il titolare delle chiavi è tenuto a sopportare le conseguenze giuridiche derivanti dall'atto posto in essere dall'usurpatore, a meno che, esperita con successo la querela di falso, riesca a dimostrare la non-appartenenza alla sua persona delle dichiarazioni contenute nel documento informatico, nel qual caso sarebbe

con la corrispondente chiave pubblica), non essendo prevista dal D.P.R. 513 alcuna forma di memorizzazione delle chiavi private presso archivi centralizzati, per un loro eventuale recupero (art. 9 lett. g)).

Altro interesse al deposito della chiave privata deriva dalla eventuale necessità di dimostrare la titolarità della chiave quando non lo si possa fare altrimenti: si pensi al caso in cui, trascorso il periodo decennale, dalla scadenza del certificato, durante il quale il certificatore è tenuto a custodire le chiavi pubbliche (art. 27, comma 3, dell'All. tec.), il titolare debba dimostrare che l'apposizione della sua firma digitale avvenne entro il periodo di validità della medesima (*rectius*: di validità del certificato). Si tratta, insomma, della possibilità di preconstituire un elemento di prova ulteriore a quello della certificazione, per la risoluzione di eventuali controversie.

Il richiamo, fatto dal terzo comma, all'applicabilità, per quanto compatibile, di quanto disposto dall'art. 605 in materia di testamento segreto, ha portato parte della dottrina¹⁰ ad escludere la necessarietà della presenza dei testimoni per la regolarità del deposito della chiave privata: infatti, il secondo comma dell'art. 7 trova una formulazione analoga a quella del primo comma dell'art. 605, con l'unica eccezione relativa alla qualità del supporto (che può assumere natura diversa dal cartaceo¹¹): mancando quindi un'espressa

tenuto "solamente" ad adempiere un'obbligazione risarcitoria derivante dall'art. 2050 c.c., richiamato implicitamente dall'art. 9 D.P.R. 513.

¹⁰ In questo senso M. MICCOLI, *Commercio telematico: una nuova realtà nel campo del diritto*, in *Dir. e Impresa*, n.3, 1997, p.487.

¹¹ L'idoneità del supporto, rimessa alla discrezione del depositante, deve essere valutata in relazione alla capacità del supporto stesso di essere racchiuso in un involucro debitamente

disposizione in merito, la presenza dei testimoni deve considerarsi rinunciabile da parte del depositante, senza che tale assenza pregiudichi la validità del deposito.

Appare, tuttavia, preferibile la tesi contraria¹² secondo cui la formulazione del secondo comma dell'art. 7 si rivela opportuna proprio per consentire la deroga alla necessità del supporto cartaceo, ritenuta imprescindibile dal primo comma dell'art. 605 c.c., rimanendo, invece, applicabile alla fattispecie *de qua* ogni altra disposizione relativa al testamento segreto compatibile con la natura della *res* depositata.

Ne deriva, quindi, non solo la necessaria presenza dei testimoni ma anche, pur in difetto di un esplicito richiamo contenuto nell'art. 7, l'applicabilità analogica dell'art. 608 c.c., che facoltizza esclusivamente il depositante al ritiro, in ogni tempo, della chiave privata presso il notaio dove essa è depositata.

L'istituto in esame pare, infine, collocabile nella previsione fatta dall'art. 61, lett. b) della L. 89/1913 (legge notarile) che regola l'obbligo di custodia del notaio relativamente agli atti presso di lui depositati per disposizione di legge o a richiesta delle parti: la dottrina maggioritaria, infatti, ritiene applicabile tale norma non solo agli atti, ma anche a carte e documenti di qualsiasi genere¹³.

sigillato da parte del notaio: deve quindi escludersi l'invio telematico di un *file* contenente la chiave privata. Così L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, op. cit., p.287.

¹² Sostenuta da G. ROGNETTA, *La firma digitale e il documento informatico*, op. cit., p. 82

¹³ Cfr. BOERO, *La legge notarile commentata*, Torino, 1993, p. 379.

9. FIRMA DIGITALE AUTENTICATA

L'autenticazione della firma digitale è disciplinata dall'art. 16 del D.P.R. 513, il quale sebbene stabilisca, al primo comma, che “si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata da notaio o da altro pubblico ufficiale autorizzato”, prevede, poi, nei commi secondo e terzo un contenuto dell'autentica digitale notevolmente diverso rispetto a quello previsto dal legislatore per l'autentica tradizionale della sottoscrizione su supporto cartaceo.

In particolare, gli unici punti di contatto con l'autentica tradizionale sono dati dall'attestazione da parte del notaio che la firma digitale è stata apposta in sua presenza previa identificazione della parte sottoscrittrice, mentre elementi di novità si rinvergono nel contenuto sostanziale dell'autentica, dovendo il pubblico ufficiale previamente verificare:

(a) *che la chiave privata con cui viene apposta la firma digitale sia valida:*

ovviamente la verifica della validità della firma digitale è la risultante della verifica del certificato corrispondente, che non deve essere scaduto, sospeso o revocato, altrimenti si produrrebbe l'effetto di una mancata sottoscrizione, come stabilito dall'art. 10 comma 5 del D.P.R.;

(b) *che il documento sottoscritto risponde alla volontà della parte;*

(c) *che il regolamento di interessi contenuto nella scrittura non sia in contrasto con l'ordinamento giuridico ai sensi dell'art. 28, primo comma, numero 1, della legge 16 febbraio 1913 n. 89 (legge notarile): ne deriva*

che il notaio non procederà all'autentica quando la scrittura contenga un regolamento di interessi proibito dalla legge, o manifestamente contrario al buon costume o all'ordine pubblico.

La previsione di questi controlli, ulteriori rispetto all'autentica tradizionale, com'è dato desumere da un rapido raffronto tra quanto dispone l'art. 16 in esame e gli articoli 2703, secondo comma, codice civile e 72, primo comma, della legge notarile¹, ha portato parte della dottrina ad affermare che “il documento informatico con firma autenticata pare porsi a *mezza via* tra la scrittura privata autenticata tradizionale e l'atto pubblico di cui agli artt. 2699 e 2700 del codice civile, quanto a efficacia probatoria”².

La questione che si pone all'interprete riguarda, in breve, lo stabilire se la funzione cui adempie l'autentica digitale sia la stessa dell'autentica tradizionale della sottoscrizione su supporto cartaceo (e cioè il raggiungimento della piena prova, fino a querela di falso, della paternità del documento) o se, invece, tale particolare forma di autenticazione abbia connotati suoi propri, che la rendono del tutto autonoma, quanto all'efficacia probatoria di cui viene investito il documento informatico, rispetto alla disciplina legislativa anteriore alla novella.

¹ L'art. 72, primo comma, della L. n. 89/1913 dispone che “l'autenticazione delle firme apposte in fine delle scritture private ed in margine dei loro fogli intermedi è stesa di seguito alle firme medesime e deve contenere la dichiarazione che le firme furono apposte in presenza del notaio e, quando decorrano, dei testi e dei fidefacienti, con la data e l'indicazione del luogo.

² Così F. DELFINI, *Forma e trasmissione del documento informatico nel Reg. ex art. 15.2 L. 59/1997*, nella rivista *I Contratti*, n.6, 1997, p. 632.

La soluzione al problema appena esposto dipenderà, ovviamente, dal considerare o meno la firma digitale, debitamente verificata *prima e fuori* del processo, come già costituente prova legale, indipendentemente dalla ricorrenza di quelle condizioni normative ritenute imprescindibili dal legislatore per attribuire questo particolare tipo di efficacia probatoria alla scrittura privata tradizionale.

Ne deriva che, a mente le conclusioni raggiunte ai paragrafi precedenti, la previsione regolamentare della necessità di un'autenticazione della firma digitale, se limitata esclusivamente all'accertamento della provenienza soggettiva del documento informatico, apparirebbe del tutto pleonastica poiché la firma digitale individua, già, con una sorta di evidenza pubblica il soggetto da cui proviene, *rectius*: da cui si presume anche legalmente provenire³, la scrittura informatica.

L'aver previsto per la firma digitale un procedimento fidefaciente più penetrante rispetto all'autentica tradizionale si armonizza, allora, pienamente con il sistema di funzionamento della crittografia asimmetrica e denuncia la consapevolezza, da parte del legislatore, della necessità di creare per la firma elettronica un procedimento autentificativo che fosse conforme alle sue caratteristiche e diverso da quello tipico della sottoscrizione su carta.

La firma digitale autenticata ex art. 16 D.P.R. 513 è, dunque, in grado di attribuire pubblica fede ad elementi rispetto ai quali, la sottoscrizione tradizionale autenticata non fornisce, invece, la stessa garanzia.

Ne deriva che la *previa* verifica della (attuale) validità della chiave privata usata per sottoscrivere, implica un controllo, da parte del notaio, relativo alla perdurante validità del certificato che, unitamente alla verifica dell'identità personale del sottoscrittore, escluderà la possibilità di un utilizzo abusivo o fraudolento del dispositivo di firma.

La previsione dell'accertamento relativo alla rispondenza tra quanto dichiarato nel documento alla volontà della parte³⁴ importa la ricognizione, da parte del pubblico ufficiale, del contenuto della dichiarazione estrinsecata nel documento e della rispondenza del dichiarato al voluto, così da escludere i vizi del volere incompatibili con tale accertamento, come l'errore; rimane esclusa, ovviamente, la violenza che potrebbe essere precedente e non contestuale all'esternazione della dichiarazione.

Infine, viene stabilita la necessità del preventivo controllo relativo alla liceità del regolamento di interessi rappresentato nel documento informatico (c.d. funzione di adeguamento).

Appare opportuno evidenziare che quest'ultima disposizione assume un'importanza del tutto particolare, poiché pone fine all'annosa questione relativa all'applicabilità del controllo di legalità previsto dall'art. 28 della L.

³³ Cfr. quanto esposto al paragrafo 3, p. 68 e ss.

³⁴ L'accertamento relativo alla volontà delle parti, dovrà essere inteso come accertamento della "volontarietà" delle dichiarazioni, cioè come volontà riferita al contenuto estrinseco delle medesime; da non confondere con volontà delle parti inerente all'intrinseco, ossia la volontà riferita al contenuto dell'atto. Il notaio non può attestarla. È opinione comune, infatti, che la simulazione relativa all'intrinseco non debba essere oggetto di querela di falso, ma possa essere provata liberamente. Cfr. MANDRIOLI, *op. cit.*, p. 190; Cons. di Stato, sez. IV, 10 luglio 1996, n. 833, fasc. 150, p. 31, Foro Amm., 1996.

89/1913 (come tale riferibile solo all'attività del notaio consistente nel ricevere atti⁵⁵) alle scritture private autenticate: la soluzione accolta dal legislatore dà, quindi, ragione alla dottrina notarile maggioritaria⁶⁶ e a quella parte di giurisprudenza che sostenevano l'estensione *de facto*⁷⁷ della portata precettiva del summenzionato articolo, in nome di una tendenziale applicabilità (in quanto compatibili) delle norme della legge notarile relative all'attività del notaio rogante atti pubblici anche all'attività del notaio che si limiti ad autenticare sottoscrizioni apposte a una scrittura privata.

Tale ultima prescrizione del secondo comma dell'art. 16 nell'affermare l'unitarietà della funzione notarile anche relativamente agli atti "solo" autenticati, in quanto dotati anch'essi di quel "crisma di ufficialità" che determina l'immissione nel commercio giuridico di convenzioni idonee a

⁵⁵ È stato, infatti, sostenuto che il divieto di ricevere atti contrari all'ordinamento giuridico richiama *in primis* gli atti pubblici, poiché solo questi ultimi sono atti del notaio in prima persona, mentre l'autenticazione costituisce un atto di "mera certificazione" dell'avvenuta sottoscrizione, distinto ed autonomo rispetto alla scrittura privata, che è un atto completamente diverso ed imputabile solo ai contraenti. Cfr. PACIFICO, *Le invalidità degli atti notarili*, Milano, 1992, pag. 276 e 547. Nello stesso senso anche Cass. Pen. 2720/1990 che precisa che il notaio non può rifiutare l'autenticazione, poiché essa non equivale a ricevere l'atto, ma consiste solo nell'esternarlo: ne deriva l'inapplicabilità dell'art. 28 della legge notarile a tale fattispecie. A ciò si aggiunga che, per interpretazione assodata, le scritture private autenticate non rientrano tra gli atti ricevuti da notaio ex art. 475 n. 3 c.p.c.: così ANDRIOLI, *Commentario al codice di procedura civile*, III, 2ª ed., Napoli 1947 e SATTA-PUNZI, *Diritto processuale civile*, 12ª ed., Padova, 1996, p. 697 ss., il primo sulla base della mancanza di "ricevimento" da parte di notaio, il secondo per l'assenza della pubblica fede propria dell'atto pubblico ex art. 2699 c.c.

⁶⁶ Si vedano BARONE, *Atto pubblico, scrittura privata e funzione notarile*, in *Vita Notarile*, 1982, p. 1459; PETRELLI, *Atto pubblico e scrittura privata autenticata: funzione notarile e responsabilità*, in *Riv. Not.*, 1994, p. 1422 e ss.; P. BOERO, *La legge notarile commentata*, Torino, 1993, p. 169 e ss.; TONDO, *Forma e sostanza dell'autentica*, in *Vita Not.*, 1980, p. 284; DI FABIO, *Manuale di notariato*, Milano, 1981, p. 189; G. CASU, *L'atto notarile fra forma e sostanza*, 1996, p. 389.

⁷⁷ In base al *principio di effettività* la norma giuridica non è la "formula" della legge ma la regola effettivamente operante nella società. In tal modo l'ordinamento sopperisce all'inadeguatezza della legislazione quando questa rimanga superata dall'evolversi della realtà socio-economica.

ingenerare affidamento ed apparenza di liceità⁸, appare, poi, quanto mai opportuna anche alla luce della “necessità di assicurare la certezza del diritto in relazione all’utilizzo di tecnologie complesse”⁹.

In quest’ottica, è interessante notare come si stia affermando nell’ordinamento statunitense la figura del *cybernotary*, la cui istituzione deriva dalla necessità di consentire al notaio appartenente ad un sistema di *common law* di svolgere compiti non più limitati a quelli di mera certificazione¹⁰, ma estesi al controllo di legalità degli atti, al fine di favorire la circolazione di questi ultimi anche nei Paesi di *civil law* senza che nascano problemi dovuti alle diverse norme che informano gli ordinamenti giuridici propri degli Stati di riferimento¹¹.

In base alle considerazioni fino a questo punto svolte, dalle peculiarità proprie dell’autentica come prevista dall’art. 16 D.P.R. 513, rispetto a quella tradizionale come disciplinata dall’art. 2703 c.c., discende questo effetto: che con la querela di falso (che abbiamo visto essere il solo strumento processuale concesso al titolare della coppia di chiavi per dimostrarsi estraneo all’emissione delle dichiarazioni contenute nel documento informatico, la prova della cui paternità risulta incontrovertibilmente

⁸ Così TONDO, *op. cit.*, p. 283.

⁹ L’affermazione è di G. ROGNETTA, *La firma digitale e il documento elettronico*, *op. cit.*, p. 130.

¹⁰ Il *public notary*, infatti, è un mero certificatore e non ha alcun dovere di verificare la conformità alla legge dell’atto che gli è sottoposto per l’autenticazione. Il primo Stato americano a prevedere l’istituzione di questa figura è stata la Florida nel 1996.

¹¹ Vedi M. MICCOLI, *Cybernotary*, in *Notariato*, 1996, p. 105 ss. Ovviamente il D.P.R. 513/97 non istituisce questa nuova figura, essendo le sue funzioni di autenticazione già proprie dell’attività notarile nostrana.

raggiunta *prima e fuori* del processo) esperibile contro il documento informatico autenticato si potrà, esclusivamente, denunciare il c.d. “falso ideologico”, cioè la mendacità dell’attestazione del pubblico ufficiale¹² o delle dichiarazioni del privato ma non l’illecito utilizzo della chiave privata utilizzata per apporre la firma digitale autenticata.

L’oggetto della querela di falso avrà, quindi, in questo caso una “latitudine sostanziale” ridotta rispetto a quella esperibile contro un documento informatico non autenticato: contro quest’ultimo, infatti, tramite querela di falso può essere denunciato, anche, l’uso abusivo della chiave privata da parte di terzi; la cui ricorrenza è, invece, necessariamente esclusa in caso di autenticazione di firma digitale ex art. 16 del D.P.R. 513.

A questo punto rimane da chiedersi come avverrà, materialmente, l’autentica di una scrittura privata informatica.

In realtà la procedura non presenta alcuna difformità rispetto a quanto già oggi avviene nella corrispondente autentica cartacea, fatte salve, ovviamente le differenze sotto il profilo tecnologico.

Il notaio redige con atto separato, ma contestuale, l’autentica informatica del documento, attestando che la firma digitale delle parti è stata apposta in sua presenza, previa verifica della loro identità ed espletamento degli altri

¹² Le possibili ipotesi di infedele autentica notarile sono state così individuate da ZAGAMI, *La firma digitale tra soggetti privati...*, op. cit., p. 923, nota 78: a) utilizzo abusivo della chiave privata di un notaio; b) infedele autentica notarile relativa a firma applicata con una chiave scaduta, revocata o sospesa con regolare pubblicazione; c) infedele autentica notarile relativa a firma applicata con una chiave valida (quindi non scaduta, revocata o sospesa), ma utilizzata da persona diversa dal legittimo titolare. Nelle due ultime ipotesi prospettate sussisterebbe anche la responsabilità civile del notaio ex art. 76 L. not.

obblighi impostigli dall'art. 16 del D.P.R., e chiude l'atto di autentica con l'apposizione della sua firma digitale, la quale "integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti" (art. 16 comma 3: è chiaro il riferimento al sigillo notarile di cui all'art. 52 della L. 89/1913).

Il fatto che la firma digitale debba essere apposta alla presenza del notaio implica che l'interessato si rechi fisicamente nello studio del pubblico ufficiale, e che qui applichi l'algoritmo di cifratura, rendendo quindi inammissibile, allo stato della normativa attuale, la possibilità di un'autentica telematica della scrittura privata digitale, a meno di ricorrere ad un sistema di videoconferenza¹³, il quale si rivela sicuramente idoneo al controllo *de quo* da parte del notaio: si potrebbe ipotizzare, allora, un previo invio telematico al notaio del *file* crittografato contenente il documento da autenticare. Il notaio appone la dichiarazione di autenticazione con la propria firma digitale nel medesimo *file* e lo rinvia all'interessato; questi procede quindi nuovamente alla crittografia e all'invio telematico a destinazione.

¹³ Le c.d. videoconferenze sono un fenomeno molto diffuso nel mondo telematico: gli utenti della rete Internet sono in grado, attraverso telecamere digitali (cosiddette webcam) e software adeguati, di essere rappresentati visivamente sul monitor di un elaboratore in un altro luogo geografico. Nel procedimento penale le videoconferenze sono state introdotte dalla legge n. 11 del 1998, che ha inserito l'art. 146 bis nelle disposizioni di attuazione del codice di procedura penale (mentre tale previsione manca del tutto nel procedimento civile). Tale articolo, dalla rubrica "partecipazione al dibattimento a distanza", dispone, al comma terzo, che "quando è disposta la partecipazione a distanza, è attivato un collegamento audiovisivo tra l'aula di udienza e il luogo di custodia, con modalità tali da assicurare la contestuale, effettiva e reciproca visibilità delle persone presenti in entrambi i luoghi e la possibilità di udire quanto vi viene detto".

Il destinatario dovrà quindi controllare una duplice provenienza: quella del documento dal mittente e quella della dichiarazione di autenticazione del notaio.

10. ATTO PUBBLICO NOTARILE DIGITALE

Il D.P.R. 513/97 sebbene attribuisca al documento informatico sottoscritto digitalmente l'efficacia probatoria della scrittura privata (art. 5) e preveda, in perfetta simmetria con la sottoscrizione tradizionale, un procedimento di autenticazione per la firma digitale (seppur con effetti del tutto peculiari - come abbiamo avuto modo di constatare al paragrafo precedente - rispetto a quanto stabilito dall'art. 2703 c.c.), nulla dispone in ordine alla redazione di un atto pubblico notarile in forma elettronica cui si ricollegli la particolare efficacia probatoria prevista dall'art. 2700 c.c.: "piena prova, fino a querela di falso, della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché delle dichiarazioni delle parti e degli altri fatti che il pubblico ufficiale attesta avvenuti in sua presenza o da lui compiuti".

La dottrina maggioritaria¹¹, interrogatasi sulla possibilità di formazione di un atto pubblico notarile digitale è giunta a conclusione sostanzialmente negativa, in base a un duplice ordine di considerazioni.

In primo luogo, osterebbe la complessità della legge notarile¹² che, agli artt. 47 ss., prescrive al notaio l'adempimento di una serie di formalità incidenti e

¹¹ Cfr. ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente "Atti, documenti e contratti in forma elettronica"*, cit., p. 915 ss.; V. FEDELI, *Documento informatico e firma digitale: valore giuridico ed efficacia probatoria alla luce del decreto del Presidente della Repubblica 10 novembre 1997, n. 513*, cit., p. 125; L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, cit., p. 294 ss.; F. DE SANTIS, *La disciplina del documento informatico. Il commento*, cit., p. 390 e in particolare nota 32; ROGNETTA, *La firma digitale e il documento informatico*, cit., p. 132; per le posizioni dottrinarie, pressoché equivalenti, della dottrina prima dell'emanazione del regolamento governativo vedi VERDE, *Per la chiarezza di idee in tema di documentazione elettronica*, in Riv. Dir. Proc., 1990, p. 715 ss.

¹² Così ZAGAMI, *Op. cit.*, p. 915.

sul contenuto dell'atto, e sull'attività di documentazione vera e propria (la presenza contestuale delle parti, dei testimoni e fidefacienti, la sottoscrizione con nome e cognome in calce all'atto notarile, la lettura del medesimo da parte del notaio con la presenza contestuale di tutti i soggetti suindicati) e sull'attività di archiviazione successiva alla formazione dell'atto pubblico (artt. 61 ss.)³³.

Alcune di queste disposizioni, poi, fanno riferimento esclusivo al “foglio”, quindi al supporto cartaceo, denunciando l'imprescindibilità di tale elemento materiale nell'attività di documentazione dell'ufficiale rogante: così, ad esempio, l'art. 51 della L. 89/13, disciplinante i requisiti dell'atto di notaio, là dove prevede, al comma 12, la necessità “negli atti contenuti in più *fogli*” della sottoscrizione delle parti, dell'interprete (qualora una o entrambe le parti non conoscano la lingua italiana), dei testimoni (se non rinunciati, congiuntamente, dalle parti ex art. 48 L. not.) e del notaio “eccettuato il *foglio* contenente le sottoscrizioni finali”.

A sostegno di tale prima argomentazione concorrerebbe, soprattutto, l'ostacolo costituito dal disposto dell'art. 12 della legge 4 gennaio 1968, n. 15 (“Norme sulla documentazione amministrativa e sulla legalizzazione e

³³ Addirittura DE SANTIS, *Op. cit.*, p. 390 nega in radice non solo la configurabilità giuridica di un atto pubblico digitale, sulla base della considerazione che “l'equiparazione della forma scritta alla forma elettronica vale per i casi in cui si debba far ricorso alla scrittura privata, non anche all'atto pubblico che – costituendo una forma documentale a sé – dovrebbe essere espressamente richiamato da quelle norme che volessero prevederne modalità di confezionamento diverse da quelle attuali”, ma, anche, la stessa legittimità di un'autentica in forma digitale ex art. 16 D.P.R., per l'esplicito contrasto che questa procedura incontra con le modalità stabilite dalla legge notarile (che richiede la redazione a mano o a macchina, la sottoscrizione di pugno del notaio e l'apposizione del sigillo), di modo che si renderebbe necessaria una “quasi totale riscrittura della legge notarile”.

autenticazione di firme”) il quale prescrive che “le leggi, i decreti, gli atti ricevuti da notai e tutti gli altri atti pubblici sono redatti a stampa, con scrittura a mano o a macchina”: tale disposizione, dalla quale si evincono i requisiti di forma dell’atto pubblico, implicherebbe che quest’ultimo si possa formare solo con un mezzo e su di un supporto tradizionali⁴.

In secondo luogo, anche a volersi ritenere superabili, da un lato, le disposizioni della legge notarile che fanno esplicito riferimento al “*foglio*” per effetto della equivalenza, sancita dall’art. 4 del D.P.R. 513, tra forma scritta e forma elettronica e, dall’altro, il disposto dell’art. 12 della L. 15/68, tramite un’interpretazione evolutiva dello stesso⁵, giungendo quindi alla positiva affermazione della configurabilità giuridica di un atto pubblico *informatico*, permarrebbe, comunque, l’impossibilità di una sua formazione *telematica* stante la disposizione dell’art. 47 legge not. che prescrive l’obbligatoria presenza delle parti davanti al notaio quale requisito di validità

⁴ Così VERDE, *Op. cit.*, p. 722. L’Autore, poi, individua in particolare alcune disposizioni della legge notarile a sostegno della sua tesi: la necessità che il notaio riceva l’atto in presenza delle parti (art. 47); la presenza di testimoni ed eventuali fidefacienti; l’attestazione che il notaio sia certo dell’identità personale dei comparenti (art.49); la menzione che il documento sia stato scritto dal notaio o da persona di sua fiducia con l’indicazione di cui consta e delle pagine scritte; la sottoscrizione del documento ad opera del notaio e delle altre parti in presenza del primo e secondo rigorose prescrizioni temporali (art. 51 ss.). In senso conforme DE SANTIS, *Op. cit.*, p. 390.

⁵ Infatti, come osservato da PETRELLI, *Op. cit.*, p. 584, la norma nasce, ovviamente, presupponendo il supporto cartaceo come materia documentale, ed in tal senso le espressioni “a stampa” e “con scrittura a mano” non lasciano dubbi né alternative. L’espressione “*a macchina*”, viceversa, consente un più ampio spettro di possibilità, essendo compatibile sia con la scritturazione su carta, sia con l’utilizzazione di un supporto magnetico o ottico, purché ciò avvenga, in entrambi i casi, mediante macchine e computer.

dell'atto pubblico altrimenti nullo per effetto dell'art. 58, comma 4, della stessa legge¹⁶.

Ne deriva, quindi, la scarsa utilità pratica di tale soluzione, “perché non sfrutta la prerogativa tipica di un sistema di firma digitale, cioè quella di evitare lo spostamento fisico delle parti interessate consentendo loro di svolgere ogni operazione anche se separate da grandi distanze. Se le parti, in altri termini, sono costrette ad andare dal notaio per assicurare la loro presenza fisica e l'indagine della loro volontà, tanto vale allora, redigere l'originale dell'atto pubblico su cartaceo...”¹⁷. Ammettere la possibilità di ricevere digitalmente un atto pubblico, si rileva quindi inutile, perché non aderente alla *ratio* del sistema di firma elettronica orientato a favorire la massima espansione della contrattazione *inter absentes*¹⁸, di modo che, escludendosi la possibilità di una sua “formazione telematica” - cioè la possibilità di documentazione dell'atto tra soggetti non presenti fisicamente nello stesso luogo -, stante il disposto dell'art. 47 l. not., risulta preferibile optare per la tesi più restrittiva sostenendosi che “non si può ritenere che l'atto pubblico informatico/telematico sia reso ammissibile...quando per la

¹⁶ Così PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, cit., p. 584-5; ROGNETTA, *Op. cit.*, p. 133; V. FEDELI, *Op. cit.*, p. 125.

¹⁷ Così ROGNETTA, *Op. cit.*, p. 133.

¹⁸ La contestuale presenza delle parti non è necessaria per la perfezione del contratto. Lo stesso codice civile, agli artt. 1326-28 e art. 1335, regola proprio le modalità di svolgimento della contrattazione a distanza (proposta-accettazione): a tali norme opera, poi, un rinvio implicito il primo comma dell'art. 12 del D.P.R. 513, dove si riproduce sostanzialmente il disposto dell'art. 1335 c.c. relativo alla presunzione di conoscenza (*rectius*: conoscibilità), incumbente sul destinatario che abbia previamente eletto domicilio elettronico nella richiesta di certificazione della propria chiave pubblica, della proposta informatica, o sua accettazione o della loro revoca,

scrittura privata autenticata, documento certamente meno rigoroso quanto a requisiti formali, è prevista dal medesimo D.P.R. una specifica e dettagliata disciplina (art. 16)⁹.

La tesi della dottrina minoritaria, sostanzialmente rinvenibile nello scritto di Petrelli¹⁰, ammette senza restrizioni la configurabilità di un atto pubblico digitale facendo leva sia su indici normativi che sull'assenza di incompatibilità tra le formalità (materiali e rituali) in cui consiste la documentazione pubblica notarile e le caratteristiche proprie del documento elettronico.

Tuttavia, sostenere, come fa l'autore sopra citato, che la possibilità di stipula dell'atto pubblico notarile digitale abbia già trovato un riconoscimento a livello legislativo non pare convincere.

Infatti, come rilevato da Albertini¹¹, non può efficacemente sostenersi la legittimità dell'atto pubblico notarile digitale dalle norme che disciplinano l'emanazione dei documenti amministrativi in forma elettronica (artt. 18-19 D.P.R. 513), in base alla considerazione che il provvedimento amministrativo, stante il disposto dell'art. 15, comma 2, della L. 59/97, è per definizione atto

quando il destinatario non riesca a dimostrare di essere stato, senza sua colpa, nell'impossibilità di averne notizia.

⁹ Così L. ALBERTINI, *Op. cit.*, p. 294.

¹⁰ Vedi PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, in Riv. Not., 1997, p. 583 ss.. L'A. pur riconoscendo che "nessun ostacolo né concettuale né normativo si oppone all'adozione della forma elettronica per l'atto pubblico notarile" non ammette, tuttavia, la configurabilità di una ricezione dello stesso in forma telematica. Cfr. anche l'articolo di D. RICCIARDI, *L'atto pubblico in forma elettronica*, pubblicato in Internet, sulla rivista giuridica on-line "Diritto & diritti", al sito www.diritto.it, il 3 dicembre 1999.

¹¹ ALBERTINI, *Op. cit.*, p. 294 nota 85.

pubblico ai sensi dell'art. 2699 c.c., in quanto redatto da pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato¹².

Bisogna infatti considerare che l'atto amministrativo è *pubblico* solamente in quanto proveniente dalla P.A.; e che quest'ultima non assume certo quella posizione di terzietà, rispetto agli interessi delle parti, caratteristica dell'ufficio notarile, nonostante la esplicita previsione del dovere di cui all'art. 97, comma 1, della Costituzione.

Si aggiunga che l'atto amministrativo, anche a voler prescindere da quanto appena detto, non partecipa sempre della medesima efficacia probatoria dell'atto pubblico notarile, il quale fa prova *fino a querela di falso* di quanto documentato dal pubblico ufficiale rogante (art. 2700 c.c.).

Quest'ultima argomentazione risulta, poi, suffragata da precise indicazioni normative. In particolare, l'art. 476 c.p., rubricato "Falsità materiale commessa dal pubblico ufficiale in atti pubblici", là dove sanziona, al secondo comma, la falsità materiale in atto pubblico "che faccia fede fino a querela di falso", denuncia, se letto *a contrario*, l'esistenza di atti pubblici che possono non essere dotati della particolare efficacia probatoria di cui all'art. 2700 c.c.¹³. Ne deriva che tra la categoria degli atti pubblici *stricto*

¹² Sul documento amministrativo elettronico *ante* legge "Bassanini-uno" vedi MINERVA, *L'atto amministrativo in forma elettronica e la sicurezza dei sistemi informativi pubblici*, in Dir. dell'Informazione e dell'Informatica, 1995, p. 939 ss..

¹³ Quanto sostenuto nel testo è stato ribadito da CASS. S.U. 11/10/1981, la quale rileva che la definizione di atto pubblico rinvenibile nel codice civile agli articoli 2699 e 2700, se applicata alla norma incriminatrice in oggetto, si rileva inadeguata: da un lato, infatti, il capoverso dell'art. 476 c.p. prevede un aggravamento di pena per il caso che la falsità concerna un atto o una parte di atto che faccia fede fino a querela di falso, con ciò ammettendo che l'ipotesi semplice di cui al comma 1 ha ad oggetto atti non fidefacienti; dall'altro lato l'art. 493 c.p. estende le norme sui

sensu e la scrittura privata esiste una terza categoria, costituita dagli atti formati nell'esercizio di una pubblica attività ma non facenti pubblica fede: questa interpretazione induce, tra l'altro, a propendere per il non ritenere decisivo il disposto dell'art. 491 *bis* c.p., introdotto dalla L. 547/93, che espressamente prevede il "documento informatico pubblico", dichiarando applicabili allo stesso le norme sul falso in atto pubblico.

Riassumendo: se le norme del D.P.R. 513 riguardanti la P.A. hanno introdotto la disciplina dell'emanazione informatica di *tutti* gli atti pubblici e non solo di quelli fidefacienti, ne discende che non è possibile individuare in tale disciplina un'identità di *ratio* sufficientemente unitaria, che la renda applicabile analogicamente agli atti pubblici provenienti da notai.

Piuttosto, appare decisiva la constatazione di una assenza di incompatibilità fra le norme della legge notarile, pensate avendo come referente il supporto cartaceo, e la stipula informatica di un atto pubblico notarile.

Infatti, l'esigenza della sottoscrizione dell'atto notarile (art. 51 n.10, legge not.) è pienamente assolta dalla apposizione della firma digitale di tutte le parti coinvolte nel procedimento: stante l'equivalenza fra i due mezzi di assunzione di paternità di un testo, sancita dall'art. 10, comma 2, del D.P.R., non vi è ragione perché l'atto pubblico si sottragga alla disciplina ivi prevista per la scrittura privata. L'assolvimento dell'obbligo di cui all'art. 52 l. not. è

falsi dei pubblici ufficiali agli impiegati incaricati di un pubblico servizio. Ne deriva, quindi, la necessità di "ricostruire in maniera *autonoma* la nozione penalistica, ampliandola fino ricomprendere tutti i documenti formati dal pubblico ufficiale o incaricato di un pubblico servizio nell'esercizio delle sue funzioni, attestanti fatti da lui compiuti o avvenuti in sua presenza

garantito dall'apposizione della firma digitale del notaio, la quale "integra e sostituisce ad ogni fine di legge la apposizione di *sigilli*, punzoni, timbri, contrassegni e marchi comunque previsti" (art. 16, comma 3, e 10, comma 6, del D.P.R. 513). Neppure costituisce ostacolo il disposto dell'art. 54 l. not., che esige la redazione dell'atto pubblico in lingua italiana, pena la nullità del medesimo (art. 58 n. 4, l. not.): la scritturazione di un documento con il linguaggio dei *bit* viene comunque tradotta sul monitor in linguaggio intelleggibile all'utente, così che il risultato raggiunto non differisce da quello prescritto dalla legge (il notaio potrà, così, adempiere l'obbligo di lettura dell'atto che, ovviamente, verrà fatta sul monitor, anziché su carta).

Non si ravvisa poi incompatibilità riguardo alle tecniche di redazione del documento notarile disciplinate dall'art. 53 l. not. e, più in generale, dall'art. 13 della l. n. 15/68^{14b}: l'inalterabilità del documento informatico è garantita in sé dall'adozione del sistema crittografico di firma digitale, in modo ancor più sicuro di quanto non avvenga per il documento cartaceo. Quanto alle postille (art. 53, comma 2, l. not.), si avrà disapplicazione della relativa disciplina per le modifiche all'atto che intervengano prima dell'apposizione delle firme digitali delle parti coinvolte nel procedimento, in quanto

ed idonei a produrre effetti giuridici". Cfr. anche M. S. GIANNINI, *Certezza pubblica*, in Enc. Dir., VI, Milano, 1960, p. 774.

^{14b} L'art 13 della legge sulla documentazione amministrativa e sulla legalizzazione e autenticazione di firme così recita: "Il testo degli atti pubblici non deve contenere lacune, aggiunte, abbreviazioni, correzioni, alterazioni o abrasioni. Sono ammesse abbreviazioni di uso comune che non lascino dubbi sul significato delle parole abbreviate. Per le variazioni da apportare al testo in dipendenza di errori od omissioni, si provvede con chiamate in calce e si cancella la precedente stesura in modo che resti leggibile.

l'immodificabilità del testo succede all'applicazione dell'algoritmo di cifratura; rispetto alle modifiche successive, invece, la disciplina *de qua* troverà applicazione con, ovviamente, le necessarie modifiche del caso: così, il notaio, dovrà associare al documento elettronico principale un documento elettronico accessorio, contenente le variazioni al contenuto del primo, e "chiuderlo" con la firma digitale sua e delle parti.

Quanto alle norme della legge notarile relative alla conservazione e rilegazione in volumi degli atti pubblici (artt. 61-66 l. not.), può dirsi che esse debbano considerarsi superate in virtù e del disposto dell'art. 15, secondo comma, della L. 59/97 (che dichiara valida e rilevante ad ogni effetto di legge, tra l'altro, "...l'archiviazione del documento elettronico con strumenti informatici") e in forza di precise e puntuali norme del D.P.R. 513 (art. 6, comma 5 e, forse, dall'art. 5, comma 2, dove si fa riferimento ad "...ogni altra analoga disposizione legislativa o regolamentare").

Le considerazioni appena svolte legittimano, dunque, appieno la configurabilità giuridica di una stipula informatica dell'atto pubblico notarile.

Esse però rischiano, al contempo, di risolversi in un mero esercizio di interpretazione giuridica, poiché rimarrebbe comunque insuperabile, ai fini di una *stipula telematica* del medesimo, l'ostacolo derivante dall'obbligo della presenza (fisica) delle parti davanti al notaio (art. 47 l. not.: obbligo che può ritenersi adempiuto solo nel caso di stipula informatica ma non telematica), la cui *ratio* va individuata, nell'obbligo gravante sul secondo di accertarsi dell'identità personale (art. 49 l. not) e d'indagare la volontà delle prime.

Il problema che si pone, insomma, è lo stesso affrontato al paragrafo precedente, riguardo alla giuridica configurabilità di un'autentica telematica delle sottoscrizioni delle parti di una scrittura privata, e medesima risulta la (possibile) soluzione.

L'obbligo gravante sul notaio di indagare la volontà delle parti e di accertare la loro identità personale potrebbe essere agevolmente adempiuto qualora tutti i soggetti partecipanti al procedimento utilizzino nei loro terminali appositi software di videoconferenza, in grado di garantire una loro presenza "virtuale" nello studio dell'ufficiale rogante: le parti, in sostanza, sarebbero fisicamente assenti ma, con l'adozione delle tecnologie opportune (e ritenendo ammissibile un'interpretazione evolutiva dell'art. 47 l. not.^{15□}), telematicamente "presenti" con la mediazione di elaboratori elettronici connessi in rete.

CAPITOLO III

^{15□} A sostegno di tale tesi potrebbe ricordarsi che la prima bozza dell'A.I.P.A. del settembre 1996 relativa a "Atti e documenti in forma elettronica", all'art. 1, secondo comma, prescriveva che: "sono esclusi dall'ambito di applicazione della presente legge gli originali degli atti pubblici notarili". Di tale divieto non è dato trovare traccia nel D.P.R. 513: il ché, potrebbe far pensare ad un ripensamento determinato dalla riconosciuta possibilità di redigere un atto pubblico notarile informatico in originale. Ma se così è, allora la strada verso il riconoscimento giuridico della possibilità di stipula telematica di un atto pubblico notarile rimane esclusivamente, e solamente, rimesso, al grado di affidabilità che le tecniche di collegamento audio-video in rete riusciranno a

ORDINAMENTO COMUNITARIO E FIRMA DIGITALE

1. ANALISI DELLA DIRETTIVA 1999/93/CE DEL PARLAMENTO E DEL CONSIGLIO, DEL 13 DICEMBRE 1999, RELATIVA AD UN QUADRO COMUNITARIO PER LE FIRME ELETTRONICHE

Il 19 gennaio 2000 è stato pubblicato nella GUCE il testo definitivo della direttiva CE relativa a un quadro comunitario per le firme elettroniche.

Si è concluso, così, l'*iter* legislativo, basato sulla procedura di codecisione (art. 251 del Trattato CE), iniziato il 13 maggio 1998 con la presentazione da parte della Commissione, su iniziativa di Martin Bangemann e di Mario Monti allora Commissari responsabili, rispettivamente, per le telecomunicazioni e per il mercato unico, di una proposta di direttiva, sulla quale erano chiamati a pronunciarsi congiuntamente il Parlamento Europeo e il Consiglio.

raggiungere, poiché, come abbiamo visto, non ci sono norme della legge notarile che denuncino una totale incompatibilità alla nascita del notaio virtuale.

Dopo una serie di emendamenti alla bozza originaria¹, riguardanti, sostanzialmente, la definizione di “firma elettronica” (i cui requisiti, nell’originaria formulazione, corrispondono ora a quelli propri della “firma elettronica avanzata”, costituendo la prima un *minus* quanto ad efficacia probatoria rispetto alla seconda), l’individuazione dei soggetti “prestatori dei servizi di certificazione” e l’introduzione di nuovi casi² in cui tali soggetti sono tenuti a rispondere per il loro operato e nei confronti del firmatario e nei confronti dei terzi che facciano affidamento sulle risultanze del certificato (qualificato), il testo definitivo della direttiva risulta composto da quindici articoli, cui seguono una serie di allegati dedicati, rispettivamente, ai “*Requisiti relativi ai certificati qualificati*” (allegato I), “*Requisiti relativi ai prestatori di servizi di certificazione che rilasciano certificati qualificati*” (allegato II), “*Requisiti relativi ai dispositivi per la creazione di una firma sicura*” (allegato III) e l’ultimo, infine, contenente una serie di “*Raccomandazioni per la verifica della firma sicura*” (allegato IV).

L’*occasio legis* è da individuarsi nella eterogeneità della legislazione interna degli Stati membri (quando presente) relativa all’utilizzo delle nuove tecnologie adibite all’autenticazione di dati: eterogeneità che potrebbe creare serie difficoltà alla comunicazione delle informazioni ed al commercio sulle reti aperte come Internet nell’ambito della Comunità Europea.

¹ Il testo integrale dell’originaria proposta di direttiva presentata dalla Commissione il 13 maggio 1998 è consultabile al sito <http://www.europa.eu.int/eur-lex/lif/index.html>. Il testo definitivo della direttiva è, invece, consultabile nell’Appendice legislativa.

² Posizione Comune del Consiglio dei Ministri dell’Unione Europea del 28 giugno 1999.

Infatti, come sostenuto nella Relazione di accompagnamento alla direttiva, “malgrado gli Stati membri sembrano concentrarsi sui medesimi problemi – in particolare, i requisiti relativi ai prestatori di servizi e ai prodotti, la condizione che le firme elettroniche debbono soddisfare per avere effetto giuridico e la struttura dei sistemi di accreditamento – è chiaro che la divergenza dei regolamenti in materia (o l’assenza degli stessi) sarà tale da ostacolare il funzionamento del mercato interno nel settore delle firme elettroniche”.

Si comprende dunque che finalità precipue della direttiva siano l’eliminazione degli ostacoli per il riconoscimento giuridico delle firme elettroniche e la libera circolazione dei servizi di certificazione: ovviamente, questi risultati sono raggiungibili solo attraverso un’armonizzazione delle discipline interne a ciascuno degli Stati membri ed il mutuo riconoscimento delle sottoscrizioni elettroniche e dei soggetti coinvolti nel sistema.

Tuttavia, è bene sottolineare come sia del tutto particolare la posizione che gli organi legislativi della Comunità europea si sono trovati ad affrontare: infatti, la materia oggetto di studio rappresenta una novità per molti degli ordinamenti degli Stati membri dell’Unione e di conseguenza per l’attività normativa del Parlamento e del Consiglio Europeo: l’obiettivo cui l’atto comunitario mira non può essere individuato nell’esigenza di armonizzare le differenti discipline statuali, o almeno lo è solo in parte, ma, piuttosto, nell’intento di dettare norme comuni per iniziare una fase legislativa nazionale nel segno dei principi disposti dagli organi sovranazionali.

Nonostante l'Italia sia stato uno dei primi paesi europei a darsi una normativa che regola in maniera completa l'utilizzo delle nuove tecnologie a scopo di autenticazione di dati, la direttiva comunitaria imporrà delle modifiche ai testi legislativi di riferimento, poiché un esame comparato fra questi ultimi e la direttiva evidenzia degli elementi di frizione che andranno eliminati in tempo utile (la direttiva dovrà essere attuata, ex art. 13, primo comma, della medesima, entro il 19 luglio 2001).

Anzitutto, è dato rilevare come la direttiva comunitaria abbia preferito adottare un impianto normativo orientato verso un sistema tecnologicamente "neutro" in quanto attribuisce validità giuridica, sia alla *firma elettronica* intesa come un qualunque mezzo di identificazione del firmatario³³, sia alla *firma elettronica avanzata* ovvero una firma sicura (art. 2, n. 1-2, e art. 5 dir. 99/93/CE).

L'intento del legislatore comunitario è, quindi, quello di non limitare alla tecnologia basata sulla crittografia asimmetrica (scelta dal legislatore italiano), la possibilità degli Stati membri di adottare strumenti diversi (forse per l'eterogeneo stato della tecnica): ciò è confermato da quanto riportato al punto 2 del capo III ("Obiettivo e campo di applicazione della direttiva") della relazione introduttiva alla originaria proposta avanzata dalla Commissione, dove si legge che "...malgrado le firme digitali realizzate tramite tecniche crittografiche siano attualmente considerate un importante

tipo di firma elettronica, il quadro di regolamentazione europeo deve essere sufficientemente flessibile da includere altre tecniche che possano essere impiegate per garantire l'autenticazione”.

La “firma elettronica avanzata” viene definita a livello comunitario (art. 2, punto 2), dir.) come “*una firma elettronica che soddisfi (cumulativamente) i seguenti requisiti:*

- a) *essere connessa in maniera univoca al firmatario;*
- b) *essere idonea ad identificare il firmatario;*
- c) *essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;*
- d) *essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati”*

Dalle norme appena riportate emerge come la disciplina italiana della firma digitale, basata sulla crittografia asimmetrica, soddisfi appieno i requisiti imposti dalla a livello CE per aversi una “firma elettronica avanzata”.

Infatti, il sistema di firma digitale nostrano garantisce che quest'ultima sia attribuita ad un solo titolare (art. 10 D.P.R. 513/97 e art 4, comma 1, dell'Allegato tecnico); idonea ad identificarlo; riferita in maniera univoca ad un solo soggetto o ai documenti cui è apposta o associata (art. 1, lett. b-f, e art. 10, comma 3, del D.P.R. 513); generata mediante un dispositivo di firma tenuto e conservato esclusivamente dal titolare (art. 4 dell'Allegato tecnico

³³ L'art. 2 dir., al punto 1), specifica che per “firma elettronica” deve intendersi qualsiasi combinazione di “dati in forma elettronica, allegati oppure connessi tramite associazione logica

che costituisce specificazione, non esaustiva, dell'obbligo di diligenza imposto dall'art. 9, comma 1, del D.P.R. 513); generata da un dispositivo di firma conforme agli standard tecnologici previsti dal d.p.c.m. 8 febbraio 1999⁴.

Piuttosto, si riscontrano elementi di difformità fra le due normative relativamente ai requisiti per poter accedere al mercato dei servizi di certificazione.

Per l'Unione, infatti, "al fine di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte, i prestatori di servizi di certificazione dovrebbero essere liberi di fornire i rispettivi servizi *senza preventiva autorizzazione*" (considerando n. 10⁵): è, così, stabilito, all'art. 3 della direttiva, che gli Stati membri *non* possono subordinare l'esercizio del servizio di certificazione ad una autorizzazione preventiva, altrimenti si ostacolerebbe lo sviluppo sia in termini di domanda che di innovazione tecnologica, ma, per raggiungere un equilibrio tra esigenze dei consumatori

ad altri dati elettronici ed utilizzata come metodo di autenticazione"

⁴ L'allegato III alla direttiva comunitaria specifica quelli che sono i *requisiti minimi* per potersi parlare di dispositivi idonei alla generazione di firme elettroniche sicure, con gli effetti, sul piano probatorio, di cui all'art. 5, comma 1, della medesima. Tali dispositivi devono garantire almeno che: a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire solo una volta e che è ragionevolmente garantita la loro riservatezza (cfr. ad esempio l'art. 1 lett. d dell'Allegato tecnico); 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 compiute con l'impiego di tecnologia attualmente disponibile; c) i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.

⁵ Viene poi specificato che "per autorizzazione preventiva non si intende soltanto qualsiasi permesso che il prestatore di servizi interessato deve ottenere dalle autorità nazionali prima di poter fornire i propri servizi di certificazione, ma anche ogni altra misura avente effetto equivalente".

ed esigenze delle imprese e conquistare la fiducia dei primi (*considerando* n. 14), lo Stato membro può subordinare la fornitura di servizi di certificazione di un elevato livello di sicurezza a *sistemi di accreditamento volontari* (comma 2).

I soggetti chiamati a svolgere l'attività di certificazione possono essere *sia persone fisiche che giuridiche* (art. 2, punto n. 11, dir.).

L'autorità di certificazione accreditata viene iscritta in un apposito albo e i certificati da essa rilasciati sono riconosciuti come dotati di un alto livello di sicurezza (il che si traduce in un maggior "grado di attendibilità" delle informazioni, relative al firmatario, contenute nel certificato medesimo) senza escludere comunque la rilevanza, la validità giuridica e la sicurezza dei certificati forniti da autorità che non hanno richiesto l'accreditamento. La distinzione si pone, quindi, solo nell'ipotesi di controversie giuridiche: le autorità di certificazione non accreditate dovranno dimostrare che i loro certificati offrono standard di autenticazione e sicurezza equiparabili ai certificati qualificati.

In particolare, i prestatori di servizi di certificazione accreditati devono essere in possesso dei requisiti previsti dall'Allegato II della direttiva e in virtù della particolare qualifica rivestita possono emettere dei certificati definiti come "qualificati", perché in grado di attribuire alla firma elettronica (avanzata) ad essi associata maggiore efficacia probatoria rispetto ad un certificato semplice: la disciplina europea distingue, infatti, tra "certificato" che è un attestato elettronico che collega i dati di verifica della firma ad una persona e

conferma l'identità di tale persona (art. 2 n. 9 dir.) e "certificato qualificato" che è un attestato elettronico conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II (art. 2 n. 10 dir.).

Contrariamente, la normativa italiana, subordina, l'esercizio delle attività di certificazione all'iscrizione in apposito elenco pubblico telematico tenuto e aggiornato a cura dell'A.I.P.A. (regime autorizzatorio: art. 8 del D.P.R. 513).

Ai fini dell'iscrizione, i soggetti richiedenti la medesima - *persone giuridiche* pubbliche o private (art. 8, comma 3, e art. 10, comma 4, del regolamento governativo) - devono presentare apposita domanda³⁶ dalla quale risulti il rispetto di tutti i requisiti previsti dall'art. 8 del D.P.R.³⁷ e dal reg. esec., pena il rigetto della medesima. La permanenza dei suddetti requisiti in capo ai certificatori è costantemente monitorata dall'A.I.P.A. e il venir meno degli stessi è causa di cancellazione dall'elenco (art. 18 d.p.c.m.), con l'effetto di produrre la caducazione degli effetti probatori connessi alle firme digitali relative ai certificati emessi dal soggetto in questione con efficacia *ex nunc*.

³⁶ Le modalità per la presentazione della domanda relativa all'iscrizione nell'elenco pubblico dei certificatori, sono state definite dall'A.I.P.A., in aderenza a quanto disposto dall'art. 16, comma 1, del d.p.c.m., con circolare del 26 luglio 1999, n. AIPA/CR/22 (Gazzetta ufficiale 2 agosto 1999, Serie Generale, n. 179) consultabile al sito <http://www.aipa.it>.

³⁷ Le persone giuridiche, pubbliche o private, che intendano esercitare l'attività di certificazione devono soddisfare, cumulativamente, i seguenti requisiti: a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria (12,5 miliardi di lire), 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 funzione 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'art. 3; d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

Questo procedimento è l'unico descritto dal Regolamento e permette il *pieno* riconoscimento giuridico alla documentazione informatica con firma digitale. Il certificatore italiano corrisponde dunque al prestatore di servizi di certificazione accreditato previsto dalla direttiva: il nostro Paese, tuttavia, non prevede una firma elettronica non basata su un sistema crittografico a chiave pubblica e la possibilità di esercitare l'attività di certificazione al di fuori del sistema di accreditamento, con gli effetti di cui all'art. 5, comma 1, D.P.R.

Inoltre il D.P.R., in contrasto con la direttiva comunitaria, non prevede l'esercizio dell'attività di certificazione (accreditata) da parte di persone fisiche o di società non rispondenti ai rigidi requisiti di cui all'art. 8 e del d.p.c.m.: ne deriva l'inevitabile e, alla luce di quanto prescrive la direttiva, ingiustificata esclusione di soggetti che potrebbero svolgere efficacemente l'attività di certificazione (qualificata) proprio per il loro ruolo e le loro funzioni tipiche, ad esempio i fornitori di accesso a Internet⁸⁰.

Ciò non esclude, tuttavia, l'impiego di firme digitali certificate da parte di soggetti non autorizzati, e l'utilizzo di sistemi di cifratura (algoritmi) diversi da quelli riconosciuti dalle regole tecniche emanate in attuazione dell'art. 3 del D.P.R. 513. In queste ipotesi, poiché il regolamento (artt. 5¹, 8¹, 2 e 3), non permette di attribuire al documento informatico l'efficacia di scrittura privata ex art. 2702 c.c., si dovrebbe rientrare, pertanto, nella generale

⁸⁰ Così CIACCI, *La firma digitale*, ed. Il Sole24ore, 1999. A tutt'oggi le società che hanno ottenuto l'iscrizione all'albo di cui all'art. 8, comma 3, del regolamento governativo sono: S.I.A. s.p.a. (dal 27 gennaio 2000); SSB s.p.a. (dal 24 febbraio 2000); BNL Multiservizi s.p.a. (dal 30 marzo 2000); Infocamere s.p.a. (dal 06 aprile 2000); Finital s.p.a. (dal 13 aprile 2000); Saritel s.p.a. (dal 20 aprile 2000); Postecom s.p.a. (dal 20 aprile 2000); Seceti s.p.a. (dal 06 luglio 2000).

categoria del semplice documento informatico, con il valore di riproduzione meccanica ex art. 2712 c.c. (art. 5, comma 2, D.P.R.): non si condividono, quindi, le affermazioni avanzate da certa parte della dottrina⁹, secondo cui la normativa italiana risulterebbe carente, rispetto a quella comunitaria, della previsione di un riconoscimento giuridico della firma elettronica semplice (art. 5, comma 2, della dir.: *“Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è: in forma elettronica, o non basata su un certificato qualificato, o non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero non creata da un dispositivo per la creazione di una firma sicura*).

La direttiva CE dispone, inoltre, che il certificato qualificato preveda l'indicazione dei limiti di responsabilità del prestatore di servizi di certificazione, dell'importo limite delle transazioni per cui il certificato è valido, ove applicabili, dello Stato di rilascio del certificato, nonché l'obbligo per i certificatori accreditati di disporre di “risorse finanziarie sufficienti... per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione”¹⁰: questi campi, pur se non espressamente

⁹ C. CIAMPI, *L'Europa verso una regolamentazione delle firme elettroniche*, articolo pubblicato il 27 ottobre 1999 sulla rivista giuridica on-line www.interlex.com; D. RICCIARDI, *L'Europa della firma digitale*, articolo pubblicato il 25 ottobre 1999 sulla rivista giuridica on-line www.interlex.com; N. MONTANARI, *La firma digitale tra normativa nazionale e normativa comunitaria*, articolo pubblicato il 7 ottobre 1999 sulla rivista giuridica on-line www.interlex.com.

¹⁰ La carenza della normativa italiana su questo punto era stata evidenziata dalla dottrina più attenta, che aveva auspicato la previsione di una copertura assicurativa obbligatoria che limitasse la responsabilità non solo del certificatore ma anche, soprattutto, del titolare della coppia di chiavi asimmetriche in caso di responsabilità per danni derivante da un utilizzo fraudolento del

previsti dal d.p.c.m 8 febbraio 1999, possono essere aggiunti senza apportare modifiche nell'elenco, non esaustivo, del dettato normativo nazionale.

Ulteriori elementi di divergenza fra normativa nazionale e comunitaria riguardano i profili internazionali della disciplina sulle firme elettroniche.

Secondo il testo comunitario, la procedura di accreditamento deve essere concepita in modo da facilitare il commercio elettronico a livello mondiale attraverso la cooperazione e il mutuo riconoscimento dei certificati emanati da autorità di certificazione di Stati non appartenenti alla Unione Europea (art.7). Le condizioni necessarie per il riconoscimento, in ogni Stato membro, dei certificati rilasciati da un prestatore di servizi di certificazione di un Paese

Terzo sono:

- a) la presenza dei requisiti previsti dalla direttiva e l'accREDITamento da parte di uno degli Stati membri; oppure
- b) la garanzia sulla validità del certificato da parte di una autorità di certificazione "europea" in possesso dei requisiti; oppure
- c) il riconoscimento dell'autorità di certificazione extracomunitaria sulla base di un accordo bilaterale o multilaterale tra l'Unione Europea e Stati terzi oppure organizzazioni internazionali.

La Commissione può intervenire per facilitare il reciproco riconoscimento dei certificati sia con proposte volte a rendere effettiva l'implementazione

dispositivo di firma, analogamente a quanto accade oggi per le carte di credito. Cfr. ZAGAMI, *La firma digitale quale fonte di certezze giuridiche*, intervento presso il convegno tenutosi a Camerino: "Documento informatico, firma digitale, commercio elettronico", 29-30 ottobre 1999, in www.unicam/ssdici/convegno_ott.html.

degli standard tecnici sia con proposte da sottoporre al Consiglio e volte ad ottenere dei mandati a negoziare accordi bilaterali e multilaterali con paesi terzi ed organizzazioni internazionali.

Contrariamente, l'art. 8, comma 4, del D.P.R. 513/97 stabilisce che nel territorio nazionale vengono riconosciuti giuridicamente validi i certificati rilasciati da certificatori, anche di Paesi terzi, operanti in base ad una licenza od autorizzazione rilasciata da uno Stato membro dell'Unione Europea o dello Spazio Economico, e solo se in possesso di equivalenti requisiti: tra questi certificatori possono essere stipulati gli accordi di certificazione previsti dall'art. 21 del d.p.c.m. 8 febbraio 1999 (c.d. accordi di *cross certification*).

I certificatori italiani possono sempre, allo stato della normativa vigente, stipulare accordi con certificatori di Paesi Terzi non accreditati da uno Stato membro, sulla base del diritto privato internazionale. Tali accordi, però, rimangono al di fuori dell'ambito di applicabilità delle disposizioni del d.p.c.m.

Un'ultima annotazione: parte della dottrina ha sostenuto l'esistenza di un'ulteriore elemento di divergenza tra normativa italiana e comunitaria. In particolare, si è sostenuto che l'art. 9 del D.P.R., pur prevedendo "tutta una serie di obblighi che devono essere adempiuti dall'Autorità di certificazione",

difetta della previsione sanzionatoria poiché non è dato “individuare eventuali responsabilità nell’ipotesi in cui tali obblighi vengano violati”¹¹.

La direttiva comunitaria, invece, supplirebbe a questa carenza individuando all’art. 6 specifiche ipotesi di responsabilità del certificatore qualificato che è tenuto al risarcimento del danno nei casi in cui venga lesa il “ragionevole affidamento” che i terzi ripongono nelle risultanze del certificato qualificato (art. 6, commi 1-2, dir.).

L’opinione non può essere accolta.

Invero, la previsione che l’art. 9, comma 2, fa circa i comportamenti positivi da adottarsi da parte del certificatore – previsione per altro non esaustiva dovendosi guardare, per espresso disposto dello stesso articolo in esame (comma 2 lett. d), anche agli obblighi imposti dal d.p.c.m. – non può disgiungersi dall’obbligo di diligenza consistente nell’*adottare tutte le misure organizzative e tecniche idonee ad evitare il danno* incombente su *chiunque* – certificatore compreso – intenda adottare un sistema di chiavi asimmetriche o della firma digitale, fissato dal primo comma.

L’aver così puntualmente specificato l’obbligo di diligenza di cui sopra, abbiamo visto essere indice della volontà del legislatore nostrano di inserire l’utilizzazione di un sistema di firma digitale nel novero delle attività pericolose di cui all’art. 2050 c.c.¹².

¹¹ In questi termini N. MONTANARI, *La firma digitale tra normativa nazionale e comunitaria*, cit.

¹² Cfr. quanto riportato a pag. 52 del paragrafo 1, capitolo II.

Non solo, quindi, la legislazione italiana individua chiare e specifiche ipotesi di responsabilità per danni del certificatore, con ciò assolvendo in pieno alle prescrizioni comunitarie sul tema (che peraltro attengono al contenuto minimo-necessario della legislazione interna), ma va oltre, prevedendo un contenuto dell'obbligo di diligenza più rigoroso di quello previsto in termini generali dall'art. 6 dir., la cui violazione non si risolve solo in un'inversione dell'onere della prova per il danneggiante: quest'ultimo infatti, una volta che il terzo dimostri il nesso eziologico tra il danno e l'attività del prestatore di servizi di certificazione, presuntivamente ritenuta pericolosa *ex lege*, non potrà liberarsi dall'obbligo risarcitorio semplicemente provando di "avere agito senza negligenza" (art. 6 comma 2 dir.) ma dovrà fornire l'ulteriore prova dell'aver adottato tutte le misure idonee ad evitare la situazione di affidamento incolpevole del terzo danneggiato.

CAPITOLO IV

CONSIDERAZIONI E VALUTAZIONI CONCLUSIVE

Con il pieno riconoscimento giuridico del documento informatico il legislatore italiano ha inteso dare ufficialmente il via a quella che è stata considerata dalla dottrina una vera e propria “rivoluzione copernicana” nell’ambito del diritto, che per il tramite del disposto dell’art. 15 della L. 59/97 e delle norme regolamentari che ne sono scaturite si presenta come la prima normativa nel panorama giuridico italiano che introduce “principi e criteri omogenei per il settore pubblico e privato, al fine di rendere meno costosa l’azione amministrativa, di agevolare lo scambio di dati e informazioni tra le pubbliche amministrazioni ed i cittadini, ed assicurare, nel settore privato, lo sviluppo dei moderni sistemi di transazione economica e documentale a tecnologia avanzata”.

“Rivoluzione”, che rischia, però, di rimanere – è proprio il caso di dirlo – solo sulla carta, o appannaggio esclusivo di una ristretta élite tecnocratica.

Quanto detto, trova conferma da una lettura non superficiale dello schema di Testo Unico sulla documentazione amministrativa che il Governo ha approvato il 25 agosto scorso.

Il testo, che dovrebbe operare una ricognizione di tutte le norme vigenti in materia di documentazione informatica al fine di una loro più rapida individuazione nel coacervo di leggi succedutesi nel tempo, sembra sortire, invece, l'effetto contrario relativamente alla materia che qui interessa. Naturalmente, fra le norme oggetto di questa attività ricognitiva, figura anche il D.P.R. 513/97 e la disciplina relativa alla firma digitale: peccato, però, che quest'opera di trasposizione di norme non sia stata svolta a dovere poiché, non solo alcune definizioni basilari del D.P.R. risultano stravolte a tal punto che ne viene persa totalmente la portata innovativa, ma a compimento dell'opera si riesce ad affermare, all'art. 75 del T.U., l'abrogazione del D.P.R. stesso.

Queste incongruenze raggiungono la loro massima espressione nell'affermazione, da un lato, che il documento informatico costituisce "rappresentazione informatica del *contenuto* di atti, fatti o dati giuridicamente rilevanti" (art. 1 del T.U.) – e quindi viene esclusa, di fatto, con l'aggiunta dell'espressione "contenuto", la possibilità di creare documenti digitali aventi valore di originale, come invece stabilito dall'art. 1 lett. a) del D.P.R. 513/97 – e, dall'altro, dalla disposizione dell'art. 2 che estende le norme concernenti i documenti informatici e la firma digitale, contenute nel capo secondo, anche nei rapporti fra privati: ne deriva che anche nei documenti privati dovrebbero essere rispettate le disposizioni in materia di formazione e conservazione dei documenti informatici delle P.A., in aperto contrasto, quindi, con quanto stabilito dall'art. 3 della Direttiva 99/93/CE, che prevede l'aggiunta di

requisiti supplementari all'utilizzo delle firme elettroniche *solo ed esclusivamente* in riferimento al settore pubblico.

Se a ciò aggiungiamo che per il Testo Unico “le modalità di produzione di atti e documenti (ivi) previste...sono utilizzate anche nei rapporti con l'autorità giudiziaria, limitatamente allo svolgimento di attività di volontaria giurisdizione” – con buona pace, quindi, di quanti idealizzavano nell'ambito della giurisdizione ordinaria un procedimento totalmente telematico – il quadro che ci si presenta risulta tutt'altro che chiaro e rende più che mai ragione a chi sosteneva che il decollo della nuova normativa fosse legato a doppio filo all'affermazione di una “*cultura giuritecnica* in cui i documenti informatici costituiscano una solida base di riferimento”, poiché l'aver sancito l'equivalenza tra documento cartaceo e informatico “rischia di rimanere una pura conquista legislativa, se non troverà un adeguato riscontro culturale nella società”.

Si vuole insomma affermare che il legislatore italiano ha creato una normativa, certamente opportuna e capace di produrre immediati vantaggi in termini economici sia nel privato che nel pubblico ma, che necessitava, forse, di un previo processo di “alfabetizzazione informatica”, a quanto pare, anche nei confronti dei c.d. “addetti ai lavori” oltre che nei confronti dei comuni cittadini: questi ultimi, peraltro, a parte i rapporti con le pubbliche amministrazioni (e anche su questo punto non pare opportuno essere troppo ottimisti), non avranno, verosimilmente, modo di giovare del nuovo strumento di firma, vuoi per la *forma mentis* degli utenti di Internet, poco

propensi a sottoporsi a regole, vuoi per le notevoli spese (le spese per la registrazione presso il certificatore, l'acquisto dell'*hardware e software* necessari che, tra l'altro, necessitano di continuo aggiornamento) che sarebbero chiamati ad affrontare per entrare a far parte, come utenti, di un sistema di firma digitale "accreditato" a fronte, tutto sommato, della conclusione di operazioni giuridiche di varia natura, ma, normalmente, non di grande valore né di intensa frequenza.

Si è parlato, a questo proposito, di "*rivoluzione elitaria*" del documento informatico per indicare il fatto che l'insieme degli oneri appena accennati sarà sopportato solo da coloro che avranno la necessità di affrontare importanti e frequenti operazioni commerciali: la normativa, in definitiva, ha un *target* abbastanza ristretto giacché diretta solo alle pubbliche amministrazioni e alle imprese medio – grandi.

A parte queste considerazioni, rimane comunque un dato indiscutibile: la disciplina dettata con il D.P.R. 513 e il collegato d.p.c.m. 8 febbraio 1999 ha il pregio di avere affrontato radicalmente e senza significative tradizioni extranazionali pregresse, che potessero fungere da linee guida, lo spinoso problema della disciplina della documentazione informatica, ma anche per avere sostanzialmente optato per l'inserimento della stessa nell'impianto vigente.

La scelta di fondo consistente nel dare rilievo giuridico alla *esclusività dell'apparato tecnico* permette di garantire, nello stesso modo e forse con più garanzie, il pieno soddisfacimento delle funzioni tipiche della sottoscrizione

tradizionale, e il tutto non mediante l'interpretazione di un segno personale dell'autore del documento, ma attraverso il meccanismo della matematica verifica dell'appartenenza al titolare di quello che è stato definito uno "strumento impersonale di attribuzione dell'identità personale dell'autore di un documento".

