FEDERICO SORRENTINO

FIRMA DIGITALE E FIRMA ELETTRONICA: STATO ATTUALE E PROSPETTIVE DI RIFORMA

PREMESSA.

Il tema della firma digitale e della firma elettronica appare particolarmente complesso: si tratta in effetti di realtà recenti, sulle quali l'analisi tecnica appare di importanza pari se non preminente rispetto all'analisi giuridica.

L'approccio della presente ricognizione è tuttavia prettamente giuridico, anche se necessariamente si dovrà dare atto, almeno in parte, dei presupposti tecnici o, *rectius*, ontologici, che sono alla base di tali nuove realtà.

La difficoltà di un'analisi giuridica che abbia la pretesa di rendere conto del quadro normativo di riferimento e dei possibili sviluppi futuri è determinata dal fatto che i nuovi strumenti di firma si inseriscono in un quadro normativo articolato e fondato su presupposti profondamente diversi, che di conseguenza mal si prestano — al fine di operare una ricostruzione organica e sistematica dell'insieme — ad innesti di istituti, i quali, pur rispondendo ad una medesima logica o finalità, sono in concreto costituiti sulla base di tecnologie completamente innovative, complesse ed interconnesse.

A prescindere dalle differenziazioni lessicali (peraltro non univoche) tra i termini « digitale » e « elettronico »[1], va comunque subito evidenziato

* Il presente testo riproduce una relazione svolta al Convegno « E-commerce - Nuove strategie di business on line » tenutosi a Milano il 15 giugno 2000.

[1] Secondo il più recente ZINGARELLI, *Vocabolario della lingua italiana*, XII ed. 1999, Bologna, il termine « digitale » è così definito: « che prevede l'uso di segnali discreti per rappresentare dati in forma di numeri o di lettere alfabetiche »; il termine « elettronica » è invece inteso come la « branca dell'elettrotecnica che studia fenomeni e applicazioni della conduzione dell'elettricità nei gas, nel vuoto e nei materiali semiconduttori ».

che la « firma digitale » è attualmente disciplinata dalla normativa nazionale (articolo 15, comma 2, della legge 15 marzo 1997, n. 59; d.P.R. 10 novembre 1997, n. 513, recante: *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 L. 15 marzo 1997, n. 59*; D.P.C.M. 8 febbraio 1999[2], recante: *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del d.P.R. 10 novembre 1997, n. 513)*, mentre la « firma elettronica » è stata oggetto di una direttiva comunitaria (Direttiva 1999/93/CE[3] del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche), che deve ancora essere recepita dall'ordinamento nazionale.

Pertanto, premessi brevi cenni sulle caratteristiche principali della « firma digitale », la successiva analisi della « firma elettronica » (comunitaria) l'implicherà imprescindibilmente la valutazione di quelle che costituiranno le prospettive più immediate di riforma dell'ordinamento nazionale in materia.

1. Inquadramento dell'istituto della firma.

Con lo sviluppo della informatica e degli strumenti telematici, e quindi del commercio elettronico e dei c.d. servizi della società dell'informazione[4], è emersa con evidenza l'esigenza di assicurare certezza ai rapporti giuridici posti in essere. Tra i connessi problemi che si pongono al riguardo vanno presi in considerazione quelli dell'esatta identificazione dei soggetti che divengono parti di tali rapporti, del modo di autenticare i dati trasmessi e di manifestare la volontà per via elettronica.

La firma digitale e la firma elettronica costituiscono una prima risposta a tali esigenze e problemi[5]. Non è irragionevole pensare infatti che il futuro

[2] Pubblicato nella *Gazz. Uff.* 15 aprile 1999, n. 87.

[3] Pubblicata in *Gazzetta ufficiale* n. L 013 del 19/01/2000 pag. 0012-0020.

[4] La definizione di « servizi della società dell'informazione » si evince, nel diritto comunitario, dalla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche (in *GU* L 204 del 21.7.1998, pag. 37). Tale direttiva è stata modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 novembre 1998, sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato (in *GU* L 217 del 5.8.1998, pag. 18 e in *GU* L 320 del 28.11.1998, pag. 54). La definizione ricopre qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione (compresa la compressione digitale) e di memorizzazione di dati, e a richiesta individuale di un destinatario di servizi; i servizi di cui all'elenco indicativo figurante nell'allegato V della direttiva 98/34/CE, non essendo forniti attraverso sistemi elettronici di trattamento e memorizzazione di dati, non sono compresi in tale definizione.

[5] Le innovazioni tecnologiche degli ultimi anni nei mezzi di comunicazione (elettroniche e informatiche) hanno indotto la dottrina a parlare di « crisi della sottoscrizione », cfr. Irti, *Idola libertatis - Tre esercizi sul formalismo giuridico*, Torino, 1985, 27; Longi, *Confezione e spedizione di documento per mezzo di terminale facsimile*, in *Giur. it.*, 1991, IV, p. 70. Da ultimo si veda C.Cost. ord, n. 117 del 2000, in cui si è affermato che costituisce « diritto vivente il principio secondo cui l'autografia della sottoscrizione è elemento essenzia-

sviluppo del commercio elettronico, se non altro nei settori ove sono in gioco tra le parti interessi economici di un certo rilievo, dipenda anche dalla efficacia e dalla sicurezza di tali nuovi strumenti. In altri termini, là dove la contrattazione tra le parti avviene nel mondo reale (cd. *off line)* senza l'uso di scritture private o addirittura tra parti anonime (anche perché generalmente il rischio economico per tali contratti è modesto), analoga contrattazione, svolta sulla rete telematica (cd. *on line*), non dovrebbe richiedere come necessario o indispensabile l'uso della firma digitale o elettronica.

Orbene per comprendere la natura e l'efficacia degli istituti giuridici della firma digitale e della firma elettronica occorre premettere alcuni concetti, quali necessari punti di riferimento dell'analisi.

Indubbiamente l'espressione « firma » si differenzia lessicalmente e giuridicamente dalla dizione « sottoscrizione », anche se spesso i due vocaboli sono usati, anche nei testi normativi, indifferentemente. In sintesi può dirsi che con il termine « firma » si indica l'impronta di segni alfabetici formanti il nome, tradizionalmente resa mediante autografia; per « sottoscrizione » si intende una firma posta nella fase finale e definitiva di uno scritto, e pertanto avente valore di manifestazione di volontà, in particolare quella di adesione al testo che la precede. Da tale distinzione discendono e si comprendono i seguenti corollari interpretativi: la « sottoscrizione » è generalmente considerata come *species* rispetto al *genus* costituito dalla « firma »[6]; il concetto di « sottoscrizione » è connesso al concetto e allo studio del « documento »[7], del quale costituisce materialmente parte integrante; la « sottoscrizione » in definitiva non è altro che l'esplicitazione della funzione — rilevante giuridicamente — dell'atto del firmare[8].

In altri termini la firma non ha generalmente rilievo o efficacia giuridica se non quando è sottoscrizione, e quindi in quanto assolva alla funzione di individuazione della provenienza e paternità di un documento[9].

---

le dell'atto amministrativo nei soli casi in cui sia espressamente prevista dalla legge, essendo di regola sufficiente che dai dati contenuti nello stesso documento sia possibile individuare con certezza l'autorità da cui l'atto proviene ». In tale pronuncia si ribadisce in sostanza quel principio generale affermato dalla dottrina, secondo il quale « requisito essenziale e sufficiente dei documenti per i quali è richiesta la sottoscrizione non è la sottoscrizione stessa, ma la possibilità di accertare concretamente la loro provenienza soggettiva », cfr. ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 152, che rinvia a MANZINI, *Il telex come mezzo di prova*, in *Giur. comm.* 1979, p. 887.

[6] In tal senso MORELLO, *Sottoscrizione*, in *Noviss. Dig. it.* XVII, Torino, 1970, p. 1004.

[7] Per un'analisi del « documento » e della bibliografia relativa, cfr. ANGELICI, « voce » *Documentazione e documento*, in *Encicl. giur. Trecc.*, XI, Roma, 1989.

[8] Con ciò si pone l'accento sull'aspetto di attestazione della conformità dello scritto al pensiero, con conseguente assunzione di paternità, e quindi sulla dichiarazione insita nella sottoscrizione, e non invece sull'*opus*, sull'operazione materiale in senso stretto (segno di inchiostro), che serve come prova documentale della dichiarazione medesima (cfr. DE SANTIS, *Natura documentale ed efficacia probatoria del telefax*, in *Riv. dir. proc.*1991, II, p. 1209).

[9] Per MORELLO, *Sottoscrizione*, in *Noviss. Dig. it.* XVII, Torino, 1970, p. 1005 è opinione generale in dottrina, fin da CARNELUTTI, *Studi sulla sottoscrizione*, in *Riv. Dir. Comm.* 1929, I, p. 509, ritenere la sottoscrizione l'elemento più importante tra quelli essenziali presenti nel documento (data, luogo, testo).

Alla luce di tali considerazioni risulta evidente la ragione per cui la firma digitale sia stata introdotta nell'ordinamento nazionale nell'ambito delle regole relative al documento informatico, e cioè con il d.P.R. 10 novembre 1997, n. 513, che è intervenuto sulla base dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59[10].

In tale contesto quindi anche la disciplina della firma digitale, pur regolata apparentemente come strumento tecnico — per fare un parallelo con un corrispondente strumento del mondo *off line*, come la penna ad inchiostro —, ha come obiettivo principale la validità e quindi l'efficacia della funzione della sottoscrizione — in quanto tale avente valore di manifestazione di volontà, in particolare quella di adesione al testo che la precede — .

2. La firma digitale secondo l'ordinamento nazionale: *a*) definizione.

Per firma digitale si intende il risultato della procedura informatica — detta 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 di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici[11].

Al di fuori di tale definizione le disposizioni vigenti, nell'ordinamento nazionale, non prevedono altre forme di firma elettronica o digitale, alle quali, pertanto, non può attribuirsi con sicurezza rilievo giuridico.

Dalla definizione sopra enunciata si evince con chiarezza che la più rilevante caratteristica e peculiarità della firma digitale, rispetto alla firma tradizionale o ad altre forme di firma elettronica, sta nel sistema di « validazione », intendendosi con ciò un sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità[12].

A differenza di quanto avviene nel mondo *off line*, nel quale il sottoscrittore tramite il possesso di una penna, può apporre la propria firma senza l'intervento di alcuno, nel mondo *on line*, come disciplinato dalle richiamate disposizioni nazionali, la sottoscrizione del documento informatico mediante l'apposizione della firma digitale richiede quindi l'intervento (per la generazione della firma stessa) di strumenti elettronici esterni (la

[10] Si riporta il comma 2 dell'articolo della legge 15 marzo 1997, n. 59: « Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge ».

[11] Cfr. la definizione data dall'articolo 1, comma 1, lettera *b*), del d.P.R. 10 novembre 1997, n. 513.

[12] Cfr. la definizione data dall'articolo 1, comma 1, lettera *c*), del d.P.R. 10 novembre 1997, n. 513. Ai sensi dell'articolo 2, comma 1, dell'allegato tecnico al d.P.C.M. 8 febbraio 1999 per la generazione e la verifica delle firme digitali possono essere utilizzati i seguenti algoritmi: *a*) RSA (Rivest-Shamir-Adleman algorithm).b) DSA (Digital Signature Algorithm). Si ricorda infatti che « criptare un testo significa applicare ad esso un algoritmo che, in relazione ad una certa variabile (chiave di criptazione), lo trasforma in un altro testo incomprensibile ed indecifrabile da parte di chi non possiede la chiave », cfr. Zagami, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 154.

chiave pubblica), verificabili da terzi e certificabili dal soggetto pubblico o privato in possesso di tali strumenti[13].

In effetti con l'espressione « chiavi asimmetriche » si fa riferimento alla coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici (viceversa un sistema *simmetrico* di criptazione è basato sull'uso di una stessa chiave per criptare e poi per decriptare[14]).

E mentre la chiave privata è conosciuta soltanto dal soggetto titolare, che se ne avvale per apporre la firma digitale sul documento informatico, la chiave pubblica è, appunto, pubblica, ed è l'elemento con il quale si verifica la firma digitale apposta sul documento informatico.

Come si vede rispetto alle componenti essenziali della firma tradizionale[15] la firma digitale è sicuramente priva del carattere dell'*autografia*, nel senso che su di essa, non essendo apposta a mano libera con caratteri grafici, non può effettuarsi alcuna analisi di corrispondenza alle caratteristiche grafiche del sottoscrittore o alla personalità del medesimo[16]; invece sicuramente potenziate sono le caratteristiche della *riconoscibilità*, in quanto essa si attua tramite il procedimento di validazione della firma e il servizio di certificazione (e non con i più incerti strumenti legati alla grafologia, come nella firma tradizionale[17]).

In realtà va ricordato che secondo la teoria tradizionale, per la validità della sottoscrizione non è sempre necessario che essa sia resa mediante « nome e cognome », essendo sufficiente una sottoscrizione anche se espressa « con un nome abbreviato o indicato con la sola iniziale » o ad anche « con le sole iniziali »[18] o addirittura anche se la stessa è indecifrabile

---

[13] Sotto tale profilo la firma digitale si avvicina ad altri strumenti utilizzati validamente come criteri idonei di imputazione di atti, quali il telegramma (la cui disciplina prevede però la consegna dell'*originale* ad un servizio pubblico come quello postale). Sullo specifico tema e per le differenze con il telex cfr. anche ANGELICI, « voce » *Documentazione e documento*, in *Encicl. giur. Trecc.*, XI, Roma, 1989.

[14] Cfr. ZAGAMI, *Firme « digitali »*, *crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 154.

[15] Sulle caratteristiche della firma cfr. MORELLO, *Sottoscrizione*, in *Noviss. Dig..it.* XVII, Torino, 1970, p. 1006.

[16] L'assenza dell'elemento dell'*autografia* nella firma digitale priva quest'ultima di quel connotato tipico della firma tradizionale, costituito dal fatto che essa è anche un « contrassegno della personalità », come l'immagine o il nome: cfr. in tal senso, con riferimento alla firma tradizionale, CANDIAN, *Documentazione e documento (teoria generale)*, in *Enc. diritto*, XIII, Milano,, 1964, p. 581. In ogni caso secondo CHIOMENTI, *Firme autografe e firme meccaniche sui titoli di credito ...e ora firme elettroniche*, in *Riv. dir. comm. e obbl.*, 1997, I, p. 727, « all'infuori di casi tassativamente imposti (che per i titoli di credito non esistono positivamente), non c'è una norma generale che richiede l'autografia » (della sottoscrizione) — cfr. la sottoscrizione meccanica prevista per i titoli azionari dall'articolo 2354, secondo comma, del codice civile — .

[17] Secondo GIANNANTONIO, *Manuale di diritto dell'informatica*, Padova, 1997, p. 397, « l'elaboratore, mentre ha, per certi versi distrutto il valore della sottoscrizione, ha, per altri versi, introdotto nuovi mezzi per controllare l'autenticità del documento; mezzi di gran lunga superiori al criterio tradizionale della sottoscrizione » (legato alla autografia).

[18] Cfr. CANDIAN, *Documentazione e documento (teoria generale)*, in *Enc. diritto*, XIII, Milano, 1964, p. 581. Anche D'ORAZI FLAVONI, *Autografia*, in *Enc. diritto*, 1959, p. 336, fa riferimento, tra le firme valide, alla « firma siglata ». Per un riscontro di diritto positivo in merito alla validità di tali sottoscrizioni cfr. articolo 8 della legge cambiaria (r.d. 14 dicembre 1933, n. 1669) od anche il secondo comma dell'articolo 602 del codice civile (sul testamento olografo).

e falsa, giacché comunque essa costituisce un elemento attraverso il quale, con qualunque mezzo, è possibile ricercarne la paternità ossia l'autore[19].

Del tutto assente nella firma digitale — essendo, per definizione, criptata — è l'elemento della *leggibilità*[20], elemento che però anche nella teoria sulla sottoscrizione tradizionale non sembra più essere assoluto, alla luce delle considerazioni che precedono[21].

2. SEGUE: *B*) SERVIZI DI CERTIFICAZIONE.

Si è detto che l'uso della firma digitale implica la possibilità di verifica della firma stessa presso un soggetto pubblico o privato che custodisce la chiave pubblica. Tale procedura dà la garanzia dell'assenza di alterazioni sul documento informatico sottoscritto, ma la reale identità del sottoscrittore[22] è data dalla « certificazione » della firma digitale.

Questa è 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)[23].

Il certificatore è quindi il soggetto pubblico o privato che custodisce le chiavi pubbliche, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati.

Salvo quanto previsto specificamente per le pubbliche amministrazioni che provvedono autonomamente (cfr. articolo 17 d.P.R. 10 novembre 1997, n. 513), i requisiti per svolgere attività di certificazione sono i seguenti: *a*) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria; *b*) possesso, da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche; *c*) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado

---

[19] Cfr. MORELLO, *Sottoscrizione*, in *Noviss. Dig. it.* XVII, Torino, 1970, p. 1012. Il segno di croce, a meno che non sia eccezionalmente previsto dalla legge, non può essere invece equiparato alla sottoscrizione neppure come idoneo a integrare il principio di prova scritta, essendo impossibile identificare l'autore del segno, cfr. CANDIAN, *Documentazione e documento (teoria generale)*, in *Enc. diritto*, XIII, Milano,, 1964, p. 581.

[20] In tal senso anche ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 157; *contra*, ma con esclusivo riferimento alle sottoscrizioni elettroniche (e quindi non necessariamente crittografate), DEL VECCHIO, *Riflessioni sul valore giuridico della sottoscrizione elettronica*, in *Riv notariato*, 1991, p. 989, secondo cui « anche la scrittura elettronica è leggibile, benché avvenga con la mediazione di strumenti artificiali ».

[21] *Contra* MORELLO, *Sottoscrizione*, in *Noviss. Dig. it.* XVII, Torino,, 1970, p. 1007, che dall'elemento della *leggibilità* argomenta una delle differenze tra sottoscrizione e firma (che ne è priva).

[22] Cfr. ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 155.

[23] Cfr. articolo 1, comma 1, lettera *h*), del d.P.R. 10 novembre 1997, n. 513.

di rispettare le norme del regolamento e le regole tecniche; *d*) qualità dei processi informatici e dei relativi prodotti, sulla base di *standard* riconosciuti a livello internazionale[24].

L'attività di certificatore può essere esercitata previa domanda di iscrizione nell'elenco pubblico previsto dall'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, domanda da inoltrarsi all'Autorità per l'informatica nella pubblica amministrazione (AIPA), che la accetta o respinge con provvedimento motivato sulla base dei requisiti del soggetto e della corrispondenza degli *standard* tecnici.

2. SEGUE: *C*) EFFICACIA DELLA FIRMA DIGITALE.

Come sopra accennato l'ordinamento nazionale assegna alla firma digitale la funzione di sottoscrizione, coerentemente con il sistema tradizionale[25]. L'articolo 10, comma 2, del d.P.R. 10 novembre 1997, n. 513 stabilisce infatti che l'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.

La funzione identificatrice (di individuazione della paternità) è garantita, come è ovvio, da disposizioni relative alla necessaria corrispondenza della firma digitale ad un solo soggetto (come espressamente stabilito dall'articolo 10, comma 3, del d.P.R. 10 novembre 1997, n. 513), ma in modo tale che il terzo sia posto in grado di controllare rapidamente tale univoca corrispondenza.

Infatti attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti con il D.P.C.M. 8 febbraio 1999, 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[26].

La sottoscrizione con firma digitale del documento informatico conferisce al documento stesso l'efficacia probatoria prevista ai sensi dell'articolo 2702 del codice civile per la scrittura privata (cfr. il disposto di cui all'articolo 5, comma 1, del d.P.R. 10 novembre 1997, n. 513). Conseguentemente il documento informatico fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, se colui contro il quale il documento è prodotto ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta[27] (secondo le norme del codice di procedura civile in tema di riconoscimento e verificazione della scrittura privata, cfr. articoli 214-220 c.p.c.[28]). Ai fini dell'efficacia

[24] Cfr. articolo 8, comma 1, del d.P.R. 10 novembre 1997, n. 513.

[25] ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 156, fa riferimento alla *funzione indicativa*, alla *funzione dichiarativa* e alla *funzione probatoria*.

[26] Cfr. articolo 10, comma 7, del d.P.R. 10 novembre 1997, n. 513.

[27] Si riporta il testo dell'articolo 2702 del codice civile: « 2702. *Efficacia della scrittura privata*. - La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. ».

[28] Per una sintetica ricognizione di tali istituti previsti nel codice di procedura civile si rinvia per tutti a CANDIAN, *Documentazione e documento (teoria generale)*, in *Enc. diritto*, XIII, Milano,, 1964,

probatoria prevista ai sensi dell'articolo 2702 del codice civile la firma digitale va intesa come strettamente correlata alla « certificazione » della firma digitale medesima[29].

Da sottolineare come, da un punto di vista sistematico, l'impostazione data alla firma digitale mediante l'equiparazione alla firma autografa di cui all'articolo 2702 del codice civile si discosti nettamente dal solco tracciato dall'evoluzione giurisprudenziale e dottrinaria tendente a dare efficacia a quegli strumenti elettronici (ad es. il telex) — diversi dal telegramma, espressamente previsto dall'articolo 2705 del codice civile —, i quali si inseriscono nell'alveo di quei mezzi, che in via eccezionale possono divenire validi criteri di imputazione (diversi dalla sottoscrizione) attraverso l'interpretazione evolutiva dell'articolo 2705 del codice civile ovvero degli articoli 2712 e 2719 del codice civile[30].

Analogamente a quanto stabilito in generale per la validità dei documenti informatici sottoscritti con firma digitale, l'articolo 11 del d.P.R. 10 novembre 1997, n. 513 ha anche disposto che i contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale sono validi e rilevanti a tutti gli effetti di legge.

Poiché nei documenti elettronici è assolutamente semplice la manipolazione e altrettanto difficile se non impossibile l'emersione di tale manipolazione o anche di correzioni apportate all'originale, la piena efficacia probatoria di documenti informatici o di contratti è assicurata proprio attraverso l'uso della firma digitale, poiché questa deve riferirsi in maniera univoca (oltre che ad un solo soggetto) al documento o all'insieme di documenti cui è apposta o associata, secondo quanto stabilito dalle regole tecniche[31].

In altri termini l'apposizione della firma digitale dovrebbe garantire non solo l'autenticità della firma stessa, ma anche — in quanto inscindibilmente legata (o associata) al documento del quale forma parte integrante

---

p. 584 e ss. Secondo ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 162, l'applicabilità dell'istituto della *verificazione* si atteggerebbe in maniera diversa con riguardo alla firma digitale, sempre e immediatamente verificabile con la procedura di « validazione ».

[29] Cfr. ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 163, che prevedeva *de iure condendo* la « certificazione » in alternativa al *riconoscimento* in giudizio di colui contro il quale il documento così sottoscritto è prodotto.

[30] Sul tema cfr. LONGI, *Confezione e spedizione di documento per mezzo di terminale fac-simile*, in *Giur. it.*, 1991, IV, p. 68; DE SANTIS, *Natura documentale ed efficacia probatoria del telefax*, in *Riv. dir. proc.*1991, II, p. 1209; nonché più di recente anche ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 152.

[31] Cfr. gli articoli 1 e 3 dell'allegato tecnico al D.P.C.M. 8 febbraio 1999, secondo i quali tale corrispondenza univoca al documento dovrebbe essere garantita dalla « funzione di hash », una funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali. Secondo il citato articolo 3 la generazione dell'impronta, che è la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash, si effettua impiegando una delle seguenti funzioni di hash, definite nella norma ISO/IEC 10118-3:1998: *a*) Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160; *b*) Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

— « *l'indelebilità* » del documento stesso, la cui manipolazione sarebbe evidenziata dalla non corrispondenza del medesimo alla firma digitale ivi apposta[32]. Al tempo stesso ciò spiega anche una delle caratteristiche attribuite alla firma digitale: la *non riutilizzabilità*[33].

L'equiparazione normativa della firma digitale alla firma autografa consente senz'altro di ritenere superata ogni perplessità in ordine all'idoneità dell'« impulso elettronico a essere forma necessaria per adempiere a quanto previsto nell'articolo 1350 del codice civile » (forma degli atti *ad substantiam*)[34].

2. SEGUE: *D*) RESPONSABILITÀ DEL CERTIFICATORE E DEL SOTTOSCRITTORE.

La normativa nazionale non detta regole espresse in tema di responsabilità del certificatore, il quale è però sottoposto al controllo da parte dell'Autorità per l'informatica nella pubblica amministrazione (AIPA), che verifica la sussistenza o il venir meno dei requisiti per svolgere tale attività, avvalendosi della collaborazione di tutte le pubbliche amministrazioni[35].

Conseguentemente chi svolge attività di certificazione sarà chiamato a rispondere del proprio operato secondo le generali regole in tema di responsabilità per inadempimento (articolo 1218 del codice civile) e, nei confronti dei terzi, in tema di responsabilità extracontrattuale (articolo 2043 del codice civile).

L'articolo 9 del d.P.R. 10 novembre 1997, n. 513 individua peraltro degli obblighi specifici a carico del certificatore, e tali obblighi indubbiamente costituiranno un parametro significativo per la valutazione dell'operato del certificatore in caso di contestazione[36].

---

[32] Secondo ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 151, « al fine dell'attribuzione di valore probatorio il supporto deve essere *indelebile* o, comunque, mantenere *traccia delle eventuali alterazioni*, in modo che qualsiasi modifica sia riconoscibile ».

[33] ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 157.

[34] LONGI, *Confezione e spedizione di documento per mezzo di terminale fac-simile*, in *Giur. it.*, 1991, IV, p. 71 che rinvia ampiamente a IRTI, *Idola libertatis - Tre esercizi sul formalismo giuridico*, Torino, 1985, 27.

[35] Cfr. l'articolo 18 dell'Allegato tecnico al D.P.C.M. 8 febbraio 1999.

[36] Secondo l'articolo 9, comma 2, del d.P.R. 10 novembre 1997, n. 513 il certificatore è tenuto a: *a*) identificare con certezza la persona che fa richiesta della certificazione; *b*) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il D.P.C.M. 8 febbraio 1999; *c*) specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite; *d*) attenersi alle regole tecniche di cui al D.P.C.M. 8 febbraio 1999; *e*) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi; *f*) attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675 (cfr. d.P.R. 318/1999); *g*) non rendersi depositario di chiavi private; *h*) procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; *i*) dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi

Nello stesso articolo 9 del d.P.R. 10 novembre 1997, n. 513, è posta una regola di condotta anche per il sottoscrittore, là dove (comma 1) stabilisce che chiunque intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. Trattasi di una clausola generale che rinvia alle regole tecniche e in particolare ai requisiti della firma digitale e al sistema di certificazione.

Sotto il profilo penale per effetto dell'articolo 491-*bis* del codice penale[37] acquistano rilievo in particolare i reati relativi alla falsità documentale: cfr. in particolare l'articolo 485 del codice penale sulla falsità in scrittura privata, ovvero la configurabilità dei più gravi delitti nel caso in cui si tratti di certificazioni o atti pubblici (la cui formazione è consentita dall'articolo 16 d.P.R. 513/1997, sulla firma digitale autenticata da notaio o altro pubblico ufficiale), tenuto conto quindi della qualità soggettiva del sottoscrittore e del contenuto del documento sottoscritto[38].

Inoltre se la falsificazione di un documento avviene intercettando comunicazioni o inserendosi in un sistema informatico o telematico si integra il concorrente delitto di cui all'articolo 617-*sexies* del codice penale[39], che riguarda più propriamente il contenuto della comunicazione.

3. La firma elettronica secondo la direttiva 1999/93/CE: *a*) definizioni.

Al fine di limitare le diversità normative negli Stati europei in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione, diversità che costituirebbero un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico, l'Unione europea ha dettato un quadro comune, applicabile a tutti gli Stati membri, relativo alle condizioni e requisiti da applicarsi alle firme elettroniche.

Anche nell'ottica europea, come nell'ordinamento nazionale per la firma digitale, la funzione della firma elettronica e dei connessi servizi di certificazione è quella diretta all'« autenticazione dei dati »[40], diretta cioè ad assicurare la provenienza e la paternità del documento.

Infatti nella direttiva 1999/93/CE la « firma elettronica » viene definita come « l'insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione »[41].

---

asimmetriche; *l*) dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.

[37] Articolo introdotto dall'articolo 3 della legge 23 dicembre 1993, n. 547.

[38] Per l'applicabilità delle norme in tema di falso documentale (falsità in scrittura privata o in atto pubblico) cfr. Giannantonio, *Manuale di diritto dell'informatica*, Padova, 1997, p. 502 e ss.

[39] Articolo introdotto dall'articolo 6 della legge 23 dicembre 1993, n. 547.

[40] Cfr. il « considerando » 4 e 8 della direttiva 1999/93/CE.

[41] Cfr. la definizione di cui all'articolo 2, n. 1 direttiva 1999/93/CE.

Tale definizione va letta in correlazione con quella di « dati per la creazione di una firma », che vengono definiti come « dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica »[42]. Inoltre il « dispositivo per la creazione di una firma » è indicato come « un software configurato o un hardware usato per applicare i dati per la creazione di una firma »[43].

Dal raffronto di tali definizioni emerge che l'ordinamento comunitario attribuisce rilievo giuridico (si veda *infra* in quali termini) a firme elettroniche, non importa se realizzate con « un software o un hardware », che utilizzano dati peculiari (codici o chiavi crittografiche private) allegati oppure connessi (tramite associazione logica) ad altri dati elettronici come « metodo di autenticazione ».

Dalle ulteriori definizioni e in particolare da quella relativa a « dati per la verifica della firma », definiti come « dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica »[44], non sembra errato ritenere che la direttiva abbia posto come requisito necessario che una firma elettronica debba essere « verificabile » (attraverso codici o chiavi crittografiche pubbliche)[45].

Inoltre viene in rilievo la definizione di « certificato », quale « attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona ».[46]

In tale generica accezione si delinea il livello minimo di firma elettronica, sulla quale è possibile effettuare un procedimento di verifica e avere una certificazione sull'identità del firmatario. In altri termini si ritiene che per la normativa comunitaria non si possa prescindere dalla stretta correlazione tra lo strumento tecnico (prodotto di firma) e il servizio di certificazione[47].

Orbene, pur non essendosi presa esplicita posizione in ordine al « come » realizzare dette chiavi crittografiche pubbliche, sembra pacifico, quanto meno allo stato della attuale tecnologia, che si tratti di chiavi di « criptazione asimmetrica » (alla quale è connesso il requisito della *non riutilizzabilità*[48]), giacché le coppie di chiavi simmetriche non sarebbero disponibili al pubblico e quindi verificabili da terzi.

Accanto alla firma elettronica come sopra definita si prevede un secondo tipo di firma elettronica, la cd. « firma elettronica avanzata ». Tale è la firma elettronica che soddisfa i seguenti requisiti: *a*) essere connessa in maniera unica al firmatario; *b*) essere idonea ad identificare il firmatario; *c*) essere creata con mezzi sui quali il firmatario può conservare il proprio

[42] Cfr. la definizione di cui all'articolo 2, n. 4 direttiva 1999/93/CE.

[43] Cfr. la definizione di cui all'articolo 2, n. 5 direttiva 1999/93/CE.

[44] Cfr. la definizione di cui all'articolo 2, n. 7 direttiva 1999/93/CE.

[45] Cfr. anche la definizione di cui all'articolo 2, n. 8 direttiva 1999/93/CE in ordine al « dispositivo di verifica della firma »: « un software configurato o un hardware usato per applicare i dati di verifica della firma ».

[46] Cfr. anche la definizione di cui all'articolo 2, n. 9 direttiva 1999/93/CE.

[47] Cfr. anche il « considerando » n. 4 direttiva 1999/93/CE: « le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati ».

[48] ZAGAMI, *Firme « digitali », crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 157.

controllo esclusivo; *d*) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati[49].

Le caratteristiche della firma elettronica avanzata e in particolare l'essere « collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati » consente di ritenere che trattasi di una firma di alta sicurezza, dovendosi garantire la cd. *indelebilità* del documento informatico sul quale è apposta.

La direttiva 1999/93/CE introduce infine un terzo tipo di firma elettronica, la « firma sicura »[50], individuato con riferimento al prodotto usato per la creazione della firma stessa: tale è il « dispositivo » che soddisfa i requisiti di cui all'allegato III della direttiva 1999/93/CE consistenti principalmente nel fatto che i dati per la creazione della firma utilizzati nella generazione della stessa devono comparire in pratica solo una volta, e non essere derivati, e che la firma deve essere protetta adeguatamente da contraffazioni, anche contro l'uso da parte di terzi[51].

Indubbiamente tali requisiti specificano e accentuano quanto previsto più genericamente per la « firma elettronica avanzata » con riferimento al requisito della riconoscibilità di ogni successiva modifica dei dati collegati alla firma stessa (cfr. articolo 2, n. 5, lettera *d*), Direttiva 1999/93/CE).

Si ritiene che il livello della « firma sicura » possa essere raggiunto da una tecnologia equivalente a quella prevista dalla « firma digitale » esistente nell'ordinamento nazionale, il quale però dovrà recepire e quindi dare rilevanza giuridica a firme elettroniche diverse e meno sicure come previsto dalla direttiva 1999/93/CE.

In ogni caso la direttiva all'articolo 3, paragrafo 7, consente agli Stati membri di assoggettare l'uso delle firme elettroniche nel settore pubblico ad eventuali requisiti supplementari; anche se tali requisiti dovranno essere « obiettivi, trasparenti, proporzionati e non discriminatori e riguardare unicamente le caratteristiche specifiche dell'uso di cui trattasi », senza « rappresentare un ostacolo ai servizi transfrontalieri per i cittadini ».

3. SEGUE: *B*) SERVIZI DI CERTIFICAZIONE.

Secondo la direttiva 1999/93/CE i servizi di certificazione possono essere forniti o da un'entità pubblica ovvero da una persona giuridica o fisica;

---

[49] Cfr. la definizione di cui all'articolo 2, n. 5, direttiva 1999/93/CE.

[50] Cfr. la definizione di cui all'articolo 2, n. 6, direttiva 1999/93/CE.

[51] Si riportano i requisiti relativi ai dispositivi per la creazione di una firma sicura, di cui all'Allegato III della direttiva 1999/93/CE: « 1. I dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che: *a*) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è ragionevolmente garantita la loro riservatezza; *b*) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro limiti ragionevoli di sicurezza, essere derivati e la firma è protetta da contraffazioni 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. 2. I dispositivi per la creazione di una firma sicura non devono alterare i dati da firmare né impediscono che tali dati siano presentati al firmatario prima dell'operazione di firma ».

infatti il « prestatore di servizi di certificazione » viene definito, dall'articolo 2, n. 11, Direttiva 1999/93/CE, come « un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche ».

Tutti i prestatori di servizi di certificazione dovranno essere liberi di fornire i rispettivi servizi senza preventiva autorizzazione. 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[52].

Tuttavia la citata direttiva lascia impregiudicata la possibilità per gli Stati membri di prevedere sistemi di accreditamento; in tal caso è necessario garantire che tali sistemi di accreditamento « non riducano la concorrenza nel settore dei servizi di certificazione »[53].

Secondo l'impostazione comunitaria sopra riportata è possibile delineare uno scenario in cui potranno liberamente operare da un lato i (semplici) certificatori e dall'altro i certificatori accreditati. Infatti è disposto chiaramente che il previsto sistema di accreditamento dovrà essere facoltativo[54].

Ma certamente il prestatore di certificazione che chiederà di essere accreditato dovrà ottenere un permesso. Infatti secondo l'articolo 2 n. 13) Direttiva 1999/93/CE l'« accreditamento facoltativo » è « qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo ».

Per i certificatori accreditati e quindi per ottenere il « permesso » suddetto dovranno essere previste dall'ordinamento nazionale, secondo la direttiva 1999/93/CE, condizioni « obiettive, trasparenti, proporzionate e non discriminatorie », ma non sarà possibile limitare il numero di prestatori di servizi di certificazione accreditati.

I certificatori della firma digitale già previsti dall'ordinamento nazionale (cfr. *supra*) si ritiene che siano compatibili con tale figura di certificatore accreditato.

I sistemi di accreditamento facoltativi saranno volti a fornire servizi di certificazione di livello più elevato[55]. In effetti la direttiva 1999/93/CE prende in considerazione diversi servizi di certificazione.

In particolare la direttiva 1999/93/CE distingue, con riferimento alle caratteristiche del servizio di certificazione, tra « certificato », quale « atte-

---

[52] Cfr. il « considerando » 10 della direttiva 1999/93/CE.

[53] Cfr. il « considerando » 12 della direttiva 1999/93/CE.

[54] Secondo il « considerando » 11 della direttiva 1999/93/CE tali sistemi (di accreditamento) « dovrebbero incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; questi ultimi dovrebbero essere liberi di aderire a tali sistemi di accreditamento e di trarne vantaggio ».

[55] Cfr. l'articolo 3, paragrafo 2, della direttiva 1999/93/CE.

stato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona »[56], e « certificati qualificati ».

Questi ultimi sono quelli che contengono i seguenti elementi: *a*) l'indicazione che il certificato rilasciato è un certificato qualificato; *b*) l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione; *c*) il nome del firmatario del certificato o uno pseudonimo identificato come tale; *d*) l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto; *e*) i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario; *f*) un'indicazione dell'inizio e del termine del periodo di validità del certificato; *g*) il codice d'identificazione del certificato; *h*) la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato; *i*) i limiti d'uso del certificato, ove applicabili; e j) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili[57].

In ogni caso tutti i certificatori — non solo quindi quelli « accreditati » — per poter rilasciare « certificati qualificati » devono essere in possesso dei seguenti requisiti: *a*) dimostrare l'affidabilità necessaria per fornire servizi di certificazione; *b*) assicurare il funzionamento di un servizio di repertorizzazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato; *c*) assicurare che la data e l'ora di rilascio o di revoca di un certificato possano essere determinate con precisione; *d*) verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato; *e*) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute; *f*) utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto; *g*) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza nel corso della generazione di tali dati; *h*) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione; *i*) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari; tali registrazioni possono essere elettroniche; j) non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave; k) prima di avviare una relazione contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e

[56] Cfr. le definizioni di cui all'articolo 2, n. 9, direttiva 1999/93/CE.

[57] Cfr. Allegato I alla direttiva 1999/93/CE.

condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile; su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato; *l*) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che: — soltanto le persone autorizzate possano effettuare inserimenti e modifiche; — l'autenticità delle informazioni sia verificabile, — i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato, — l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza[58].

Infine sono previsti, come raccomandazioni (quindi non a carattere vincolante), requisiti ulteriori sulla procedura di verifica della firma (cfr. Allegato IV Direttiva 1999/93/CE).

3. SEGUE: *C*) EFFICACIA DELLE FIRME ELETTRONICHE.

La direttiva 1999/93/CE, nell'affrontare il problema dell'efficacia giuridica da attribuire alle firme elettroniche, ha premesso l'estraneità di tale tema rispetto alla tematica della conclusione ed esecuzione dei contratti, ovvero ad altre formalità di natura extracontrattuale concernenti l'apposizione di firme[59].

Altrettanto chiaramente è stato enunciato l'obiettivo di dare rilievo alle firme elettroniche ai fini dell'ammissibilità come mezzo probatorio nei procedimenti giudiziari[60].

In tale contesto l'articolo 5 della direttiva 1999/93/CE ha disposto come segue: « 1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura: *a*) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e *b*) siano ammesse come prova in giudizio. 2. 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 ».

Da tale disposizione si evincono due livelli di efficacia *probatoria*. Il primo livello, quello garantito dalle firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura, è di completa equiparazione giuridica alle firme

[58] Cfr. l'articolo 2, n. 10, e l'Allegato II, direttiva 1999/93/CE.

[59] Cfr. il « considerando » 17 della direttiva 1999/93/CE .

[60] Cfr. il « considerando » 16 della direttiva 1999/93/CE.

autografe se siano rispettati i requisiti per le firme autografe[61] e se vi sia stata l'ammissione in giudizio.

Alla luce di tali premesse si ritiene che come già stabilito per la firma digitale sopra menzionata, il legislatore nazionale, nel recepire la direttiva 1999/93/CE, stante l'equiparazione alla firma autografa in forza del disposto del primo paragrafo dell'articolo 5, paragrafo 1, della direttiva 1999/93/CE, dovrà stabilire che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura costituiscono « piena prova » ai sensi dell'articolo 2702 del codice civile, e che, di conseguenza, esse soltanto sono idonee alla stipula di atti che richiedono la forma scritta *ad substantiam* (e cioè come elemento di validità della dichiarazione di volontà e quindi del documento medesimo).

Come per l'articolo 5, comma 1, d.P.R. 10 novembre 1997, n. 513 il richiamo all'« efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile »[62] dovrebbe essere sufficiente a garantire il rispetto degli altri requisiti e presupposti di ammissibilità della prova previsti dallo stesso articolo 2702 del codice civile (riconoscimento della sottoscrizione) e dalle corrispondenti norme del codice di procedura civile (in tema di riconoscimento e verificazione della scrittura privata, cfr. articoli 214-220 c.p.c.).

In base al disposto del paragrafo 2 dell'articolo 5 della direttiva 1999/93/CE si pone il problema dell'efficacia delle altre firme elettroniche e cioè della firma elettronica certificata (cfr. *supra sub* 3. *a*), ma non basata su un certificato qualificato, della firma elettronica basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione non accreditato, ovvero della firma elettronica non creata da un dispositivo per la creazione di una firma sicura.

Non essendovi per tali firme l'equiparazione alla firma autografa, l'ammissibilità delle stesse come prova in giudizio non sarà come « piena prova » (ai sensi dell'articolo 2702 del codice civile), ma su un piano di più ridotta efficacia, come « prova semplice », valutabile liberamente, e quindi anche contestabile validamente con qualsiasi mezzo, senza necessità di ricorrere alle forme della querela di falso nei confronti del sottoscrittore che la disconosce.

In altri termini il documento informatico sottoscritto con semplice firma elettronica secondo la direttiva costituisce, dal punto di vista probatorio, principio di prova per iscritto, apprezzabile in base al libero convincimento del giudice (articolo 116 del codice di procedura civile)[63], e quindi tale da giustificare su tale documento l'ammissibilità di prove testimoniali (cfr. articoli 2721 e 2724 del codice civile)[64].

---

[61] Cfr. anche il « considerando » 20 della direttiva 1999/93/CE.

[62] Si riporta l'articolo 5, comma 1, d.P.R. 10 novembre 1997, n. 513 — avente come rubrica l'espressione: *Efficacia probatoria del documento informatico* —: « Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile. ».

[63] Ai sensi del « considerando » 21 della direttiva 1999/93/CE la direttiva medesima « non lede e norme nazionali in materia di libero uso delle prove in giudizio ».

[64] Ciò in linea con quanto già sostenuto, anche se con generico riferimento al documento elettronico, da GIANNANTONIO, *Manuale di diritto dell'informatica*, Padova, 1997, p. 396 e ss.

3. SEGUE: *D*) RESPONSABILITÀ DEL CERTIFICATORE E DEL SOTTOSCRITTORE.

Va premesso che la direttiva 1999/93/CE prevede un controllo da parte di organismi pubblici o privati sui prestatori dei servizi di certificazione[65].

Come già sopra osservato, nell'ordinamento nazionale si è già effettuata la scelta di affidare il controllo dei certificatori ad un'autorità amministrativa indipendente (l'AIPA) e quindi ad un organismo pubblico. Nel recepire la direttiva 1999/93/CE sarà però teoricamente possibile optare anche per un sistema di controllo dei certificatori affidato a soggetti privati, anche se a tale opzione si oppone necessariamente l'esigenza di salvaguardare le esperienze già acquisite su tale settore. D'altra parte la diffusione di certificatori non accreditati potrà porre il problema delle risorse economiche disponibili a garantire l'efficienza del controllo affidato ad un unico organo pubblico.

In ordine alla responsabilità dei certificatori la direttiva 1999/93/CE detta una norma *minimale* (nel senso che gli Stati membri potranno prevedere forme di responsabilità più severe).

Tale norma è prevista per i certificatori che rilasciano un certificato qualificato; essi dovranno rispondere dei danni provocati a entità o persone fisiche o giuridiche che facciano ragionevole affidamento su detto certificato circa l'esattezza di tutte le informazioni contenute nel certificato qualificato a partire dalla data di rilascio e il fatto che esso contenga tutti i dati prescritti per un certificato qualificato, nonché circa la garanzia che, al momento del rilascio del certificato, il firmatario identificato nel certificato qualificato detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato; ed infine circa « la garanzia che i dati per la creazione della firma e i dati per la verifica della firma possano essere usati in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi entrambi » ovvero « per la mancata registrazione della revoca del certificato »[66].

Chiarito l'oggetto della responsabilità l'articolo 6 della direttiva 1999/93/CE prevede inoltre una regola in materia di prova che tende a favorire il danneggiato. Si prevede infatti l'inversione dell'onere della prova circa la valutazione della colpa del certificatore in ordine alle riscontrate inesattezze del certificato qualificato che siano state fonti di danno. In effetti il prestatore di servizi di certificazione è esonerato da tale responsabilità solo se « prova di aver agito senza negligenza »

Nell'ordinamento nazionale tale disposizione è sostanzialmente conforme alla regola generale in tema di inadempimento delle obbligazioni (articolo 1218 del codice civile), mentre costituisce un'eccezione rispetto alla regola generale di responsabilità aquiliana (articolo 2043 del codice civile), nella quale il danneggiato deve provare anche la colpa di chi ha provocato il danno.

Altre disposizioni sono dettate in considerazione del fatto che il certificato qualificato può contenere dei limiti d'uso e limiti del valore dei negozi

[65] Cfr. il « considerando » 13 e articolo 3, paragrafi 3 e 4, direttiva 1999/93/CE.

[66] Cfr. espressamente l'articolo 6 direttiva 1999/93/CE.

per i quali il certificato può essere usato. In tali casi, qualora detti limiti siano riconoscibili dai terzi, il prestatore di servizi di certificazione sarà esentato dalla responsabilità per i danni derivanti dall'uso di un certificato qualificato che ecceda i limiti suddetti.

Per quanto riguarda la posizione del sottoscrittore la direttiva non detta regole specifiche. Si pone in ogni caso il problema se la fattispecie delittuosa di cui all'articolo 491-*bis* del codice penale, che richiama i reati sulla falsità nei documenti informatici, possa ritenersi direttamente applicabile a fattispecie di falso derivanti dall'apposizione delle firme elettroniche previste dalla direttiva 1999/93/CE una volta che queste saranno recepite nell'ordinamento nazionale ovvero se sia comunque necessaria una nuova e autonoma norma incriminatrice, in ossequio al principio di stretta legalità sancito dall'articolo 1 del codice penale (e dall'articolo 25, secondo comma, Cost.).

Innanzitutto su un piano di uniformità di trattamento non v'è dubbio che l'equiparazione alla firma autografa imponga un'equiparazione anche delle connesse responsabilità penali in caso di falsificazioni connesse all'apposizione delle firme elettroniche (come già osservato per la firma digitale).

In secondo luogo deve considerarsi che la nozione di « documento informatico », contenuta nell'articolo 491-*bis* del codice penale, comprende « qualsiasi dato o informazione avente efficacia probatoria ».

Conseguentemente si tratta di un reato nel quale sono ipotizzate più condotte che hanno come risultato la falsificazione del documento informatico. Pertanto, così come si è ritenuto che nella fattispecie di cui all'articolo 491-*bis* del codice penale possa senz'altro essere compresa la condotta consistente nella falsificazione della firma digitale (alla quale è stata attribuita efficacia probatoria nel 1997 e quindi successivamente all'entrata in vigore del citato articolo 491-*bis* del codice penale, introdotto dall'articolo 3 della legge 23 dicembre 1993, n. 547), nella suddetta fattispecie criminosa dovrebbe essere compresa anche la condotta di falsificazione delle firme elettroniche quando ad esse l'ordinamento nazionale attribuirà efficacia probatoria, senza necessità di un'ulteriore norma *criminis*.