Firma elettronica

Attuazione della direttiva europea sulla firma elettronica, ovvero la forma «sine probatione»

In sede di attuazione della direttiva europea sulla firma elettronica, il legislatore delegato italiano, senza che la direttiva lo richiedesse né che la legge delega lo autorizzasse, sembra aver introdotto nel nostro ordinamento un'inedita "forma *sine probatione*"

DECRETO LEGISLATIVO 23 gennaio 2002 n. 10
Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche

(G.U. n. 39, 15 febbraio 2002, Serie Generale)

IL PRESIDENTE DELLA REPUBBLICA
(omissis)
Emana
il seguente decreto legislativo:

Art. 1.

1. Il presente decreto reca le disposizioni legislative per il recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

Art. 2.

1. Ai fini del presente decreto si intende per:

a) "firma elettronica" l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

b) "certificatori" coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche;

c) "certificatori accreditati" i certificatori accreditati in Italia ovvero in altri Stati membri dell'Unione europea, ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE;

d) "certificati elettronici" gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;

e) "certificati qualificati" i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva;

f) "dispositivo per la creazione di una firma sicura" l'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti di cui all'articolo 10;

g) "firma elettronica avanzata" la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

h) "accreditamento facoltativo" il riconoscimento del possesso, da parte del

certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Art. 3.

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva.

2. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, di seguito denominato: "Dipartimento", svolge funzioni di vigilanza e controllo nel settore, anche avvalendosi dell'Autorità per l'informatica nella pubblica amministrazione e di altre strutture pubbliche individuate con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri interessati.

Art. 4.

1. I certificatori stabiliti in Italia che intendono rilasciare al pubblico certificati qualificati devono darne avviso, anche in via telematica, prima dell'inizio dell'attività, al Dipartimento.

2. I controlli volti ad accertare se il certificatore che emette al pubblico certificati qualificati soddisfa i requisiti tecnici ed organizzativi previsti dal regolamento di cui all'articolo 13 sono demandati al Dipartimento, che all'uopo può avvalersi degli organismi indicati nell'articolo 3, comma 2.

3. I controlli di cui al comma 2 sono effettuati d'ufficio ovvero su segnalazione motivata di soggetti pubblici o privati.

Art. 5.

1. I certificatori che intendono conseguire dal Dipartimento il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati.

2. Il richiedente deve essere dotato di ulteriori requisiti, sul piano tecnico, nonché in ordine alla solidità finanziaria ed alla onorabilità, rispetto a quelli richiesti per gli altri certificatori ai sensi del regolamento di cui all'articolo 13.

3. Il Dipartimento, per il vaglio delle domande presentate ai sensi del comma 1, può avvalersi degli organismi indicati nell'articolo 3, comma 2.

4. Quando accoglie la domanda, il Dipartimento dispone l'iscrizione del richiedente in un apposito elenco pubblico, consultabile anche in via telematica, tenuto dal Dipartimento stesso.

Art. 6.

1. L'articolo 10 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, approvato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:

"Art. 10 (L). (Forma ed efficacia del documento informatico). - 1. Il documento informatico ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate.

2. Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

4. Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa

del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

5. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su di un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Comunità europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e Paesi terzi o organizzazioni internazionali.

6. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro dell'economia e delle finanze.".

Art. 7.

1. Dopo l'articolo 28 del testo unico emanato con il decreto del Presidente della Repubblica n. 445 del 2000 è aggiunto il seguente:

"Art. 28-bis (L). (Responsabilità del certificatore). - 1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento:

a) sull'esattezza delle informazioni in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;

b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;

c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato, salvo che provi d'aver agito senza colpa.

3. Il certificatore può indicare, in un certificato qualificato, i limiti d'uso di detto certificato ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.".

Art. 8.

1. All'articolo 36 del testo unico emanato con il decreto del Presidente della Repubblica n. 445 del 2000 il comma 1 è sostituito dal seguente:

"1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica, del documento d'identità elettronico e della carta nazionale dei servizi sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali.".

2. All'articolo 36 del testo unico emanato con il decreto del Presidente della Repubblica n. 445 del 2000, al comma 3 la lettera e) è sostituita dalla seguente:

"e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.".

3. All'articolo 36 del testo unico emanato con il decreto del Presidente della Repubblica n. 445 del 2000 i commi 4 e 5 sono sostituiti dai seguenti:

"4. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate ai fini dei pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con decreto del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

5. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi.".

Art. 9.

1. All'articolo 38 del testo unico emanato con il decreto del Presidente della Repubblica n. 445 del 2000, il comma 2 è sostituito dal seguente:

"2. Le istanze e le dichiarazioni inviate per via telematica sono valide:

a) se sottoscritte mediante la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura;

b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (L).".

Art. 10.

1. La conformità dei dispositivi per la creazione di una firma sicura ai requisiti prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Lo schema nazionale non reca oneri aggiuntivi per il bilancio dello Stato ed individua l'organismo pubblico incaricato di accreditare i centri di valutazione e di certificare le valutazioni di sicurezza. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

2. Il decreto di cui al comma 1 fissa la data sino alla quale per l'accertamento di cui al comma stesso si procede in base al regime transitorio previsto dall'articolo 63 delle regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici stabilite, ai sensi dell'articolo 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato nella Gazzetta Ufficiale n. 87 del 15 aprile 1999, e prorogato, da ultimo, con il decreto del Presidente del Consiglio dei Ministri 3 ottobre 2001, pubblicato nella Gazzetta Ufficiale n. 233 del 6 ottobre 2001.

3. La conformità dei dispositivi per la creazione di una firma sicura ai requisiti prescritti dall'allegato III della direttiva 1999/93/CE è inoltre riconosciuta se certificata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva stessa.

Art. 11.

1. I documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori iscritti nell'elenco pubblico tenuto dall'Autorità per l'informatica nella pubblica amministrazione ai sensi dell'articolo 27, comma 3, del testo unico approvato con il decreto del Presidente della Repubblica n. 445 del 2000, producono gli effetti previsti dagli articoli 6, capoversi 1°, 2° e 3°, e 9 del presente decreto.

2. I certificatori che, alla data di entrata in vigore del regolamento di cui all'articolo 13, risultano iscritti nell'elenco pubblico previsto dall'articolo 27, comma 3, del testo unico

approvato con il decreto del Presidente della Repubblica n. 445 del 2000, sono iscritti d'ufficio nell'elenco pubblico previsto dall'articolo 5 del presente decreto, ed hanno facoltà di proseguire l'attività già svolta o di iniziarne l'esercizio, se non precedentemente avviato, con gli effetti di cui al comma 1 del presente articolo.

3. Sino alla data di entrata in vigore del regolamento di cui all'articolo 13, i certificatori di cui all'articolo 4 sono tenuti all'osservanza delle disposizioni dell'articolo 28, comma 2, lettere a), c), e), f), g), h) ed i), del testo unico approvato con il decreto del Presidente della Repubblica n. 445 del 2000. In caso di cessazione dell'attività, devono darne preventivo avviso al Dipartimento, comunicando contestualmente la conseguente rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa.

Art. 12.

1. Le disposizioni vigenti alla data di entrata in vigore del presente decreto che consentono di presentare per via telematica istanze o dichiarazioni alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi secondo procedure diverse da quelle indicate nell'articolo 9 continuano ad avere applicazione fino alla data fissata, con riferimento ai singoli settori, con decreto del Presidente del Consiglio dei Ministri, da adottarsi, di concerto con i Ministri interessati, entro il 30 novembre 2002. La suddetta data non può comunque essere posteriore al 31 dicembre 2005.

Art. 13.

1. Entro trenta giorni dalla data di entrata in vigore del presente decreto è emanato un regolamento ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, anche ai fini del coordinamento delle disposizioni del testo unico emanato con il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, con quelle recate dal presente decreto e dalla direttiva 1999/93/CE, nonché della fissazione dei requisiti necessari per lo svolgimento dell'attività dei certificatori.

2. Il regolamento è emanato su proposta e con il concerto dei Ministri indicati nell'articolo 1, comma 2, della legge 29 dicembre 2000, n. 422. Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

IL COMMENTO
di Ugo Bechini e Mario Miccoli

Il debutto della firma digitale nella nostra legislazione, avvenuto nel 1997 [1], fu caratterizzato da un approccio monistico. Si disciplinò un modello unitario di firma digitale, provvisto delle più elevate caratteristiche di sicurezza consentite dalle tecnologie disponibili; la chiameremo firma digitale *tout court*, secondo un uso ormai diffuso, per distinguerla dalla più generale nozione di firma elettronica, su cui torneremo tra breve.

La firma digitale

La firma digitale ha la funzione di garantire la provenienza del documento sottoscritto, l'immutabilità del documento stesso e la possibilità per chiunque di procedere alla verifica obiettiva della firma, ovunque nel mondo ed in tempo reale. Sul fronte opposto, richiede strutture e procedure complesse e relativamente costose, sia in fase di rilascio del certificato di firma che di manutenzione del sistema. La firma digitale propriamente detta è quindi lo strumento

---

1 Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (*Gazz. Uff.* n. 60 del 13 marzo 1998).

d'elezione per la circolazione telematica di documenti che richiedono un elevato livello di sicurezza; di qui, tra l'altro, l'attenzione del mondo del notariato 2, che in Italia si sta concretizzando in questi mesi con la nascita di una apposita *Certification Authority* in seno al Consiglio Nazionale del Notariato. Su questo fronte non vi è motivo di ripensamento alcuno; il "tradimento", paradossalmente ma non troppo, è venuto dal mondo dell'impresa. Del documento elettronico si parla da una decina di anni e ogni volta si sottolinea il fatto che entro breve tempo, il commercio elettronico, il suo utilizzo, la documentazione dei contratti *paperless*, diventerà un fatto mondiale, un fenomeno inarrestabile, una valanga senza limiti. Nulla di tutto ciò è accaduto e, a ben vedere, la cosa non deve sorprendere.
La firma digitale si è rivelata per lo più inutile nelle grandi transazioni, ove le carenze sul fonte

---

2

Che ha dato origine ad una copiosa letteratura, tra cui: Maria Claudia Andrini, *Dal tabellione al sigillo elettronico*, in *Vita notarile*, 1998, p. 1787 ss.; **Danilo Giaquinto e Paola Ragozzo,** *Il sigillo informatico*, in *questa Rivista*, 1997, p. 80 ss; **Enrico Maccarone,** *Documento informatico e firma digitale*, in *C.N.N. Attività*, ottobre 1997, p. 57 ss.; *Introduzione alla firma digitale* (con Manlio Cammarata) http://www.interlex.it/docdigit/intro/indice.htm; *Commentario* (con Cesare Massimo Bianca ed altri) *al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 633 ss; **Michele Nastri,** *La firma digitale*, in *Noter - Notariato dell'Emilia Romagna*, n. 7, gennaio/giugno 1999, p. 9 ss.; *L'adempimento unico informatico*, in *Federnotizie*, marzo 2001 http://www.federnotizie.org/2001/marzo/nastri.htm ; **Gaetano Petrelli,** *Documento informatico, contratto in forma elettronica e atto notarile*, in *Notariato*, 1997, p. 567 ss.; *Regolamento sugli atti, documenti e contratti in forma elettronica*, in *Notariato*, 1998, p. 294 ss.;**Paolo Piccoli e Giovanna Zanolini,** *Il documento elettronico e la "firma digitale"*, in *Rivista del Notariato*, 2000, p. 879.; **Raimondo Zagami,** *Firme "digitali", crittografia e validità del documento elettronico*, in *Diritto dell'informazione e dell'informatica*, 1996, p. 151 ss.; *La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica"*, in *Diritto dell'informazione e dell'informatica*, 1997, p. 903 ss.; *Firma digitale e sicurezza giuridica*, Padova, 2000; *La firma digitale*, Relazione scritta per la pubblicazione negli atti del Convegno organizzato da ITA sul tema "La firma digitale", Milano 15 /16 novembre 2001, http://web.tiscali.it/conoge/zagami.pdf . Sia consentito far pure riferimento a nostri precedenti lavori: **Mario Miccoli,** *Cybernotary*, in *questa Rivista*,

della sicurezza sono ovviate da una conoscenza reciproca dei contraenti. Si prendano ad esempio i trasferimenti di denaro da una banca all'altra: sia le banche come persone giuridiche, sia i loro funzionari, si conoscono perfettamente, posseggono reti telematiche la cui sicurezza è assicurata non da tecniche crittografiche, ma dalla cosiddetta trasmissione punto a punto: la sicurezza viene dunque garantita a livello hardware anziché software, e comunque sussiste uno specifico sistema di garanzie reciproche, che rende il documento elettronico del tutto superfluo oppure, al più, un elemento puramente addizionale di protezione.
Sul fronte opposto, quello delle piccole transazioni quotidiane in Rete, quasi mai è realmente necessario il livello di sicurezza offerta dalla firma digitale [3]. Un'operazione delle più comuni, come l'acquisto via Internet di un biglietto aereo, può accontentarsi di molto meno: ad esempio del sistema SSL, ormai diffusissimo in Rete. Tutto ciò che SSL può fare è assicurare l'utente di essere davvero in comunicazione con il server da lui prescelto, e che i dati in transito non possono agevolmente essere letti da terzi. Le lacune sono evidenti: il server della compagnia aerea non ha affatto la certezza di essere in contatto con quel determinato utente [4], e non vi è alcuna forma di documentazione obiettiva del contenuto delle comunicazioni scambiate [5]. Il sistema quindi non offre molto: quanto basta però a convincere l'utente non troppo prevenuto a digitare con serenità il numero della propria carta di credito, nella ragionevole certezza che solo il computer della compagnia aerea potrà leggerlo. Se le comunicazioni sono intercettate, in verità, ad un esperto non è impossibile [6] violare il sistema SSL e leggere il numero della carta di credito: tenendo conto però che in genere il numero stesso è ben lungi dall'essere un segreto di stato, noto com'è

1996, p. 105 ss.; *Commercio telematico: una nuova realtà nel campo del diritto*, in *Diritto e Impresa*, 3, 1997, 487 ss; *Documento e commercio telematico – Guida al regolamento italiano (dpr 513/97)*, IPSOA, 1998; Ugo Bechini: *Vademecum minimo in tema di funzione notarile e firma digitale*, in *Rivista del Notariato*., 2000, p. 1155 ss.; *Contiene atto notarile: per la data di scadenza vedere sul tappo*, in *Federnotizie*, maggio 2001 - http://www.federnotizie.org/2001/maggio/bechin.htm; *Quando la smart card diventa un souvenir*, *Interlex*, 21 settembre 2001, http://www.interlex.it/docdigit/bechini1.htm.

3 In tal senso già Michele Nastri, *La firma digitale*, cit. Non sembra invece cogliere tale prospettiva differenziata il documento in materia di firma elettronica approvato due anni più tardi dalla CNUE, Conferenza dei Notariati dell'Unione Europea (Roma 8 dicembre 2001).

4 Questa possibilità è teoricamente contemplata dal protocollo SSL, ma è di regola inutilizzata.

5 Warwick Ford e Michael S. Baum, *Secure Electronic Commerce*, Upper Saddle River (New Jersey, USA) 2001, p. 159.

6 I ragguagli forniti al proposito dai produttori, che invariabilmente misurano il tempo occorrente per violare i loro sistemi in settimane, mesi ed anni (anche migliaia di anni) di lavoro di un supercomputer, si

ad intere legioni di negozianti, albergatori, ristoratori e relativi dipendenti, anche questa approssimativa sicurezza può risultare in definitiva del tutto proporzionata alla bisogna.
Non solo. Livelli di insicurezza che in altri contesti potrebbero risultare insopportabili, nel mondo dell'*e-commerce* sono, al contrario, facilmente gestibili [7]. Nella stragrande maggioranza dei casi, è sufficiente l'intervento di un terzo, il gestore della carta di credito: questi garantisce il pagamento, assumendosi nei confronti del venditore tutti i rischi di insolvenza delle transazioni. Ciò è reso possibile da due fattori concomitanti: l'ammontare singolo di ogni transazione è accettabilmente basso ed il numero di esse è incredibilmente alto. Anche laddove un non trascurabile numero di esse non vada a buon fine, il gestore della carta di credito può quindi sopportare l'onere del rimborso del prezzo non corrisposto dal cliente finale. Un approccio di tipo statistico, dunque, evidentemente impensabile nell'ambito di transazioni immobiliari o nella gestione degli ordini di cattura.

La Direttiva 93/1999

In questo panorama si inserisce la Direttiva 93/1999 [8] che, a differenza della previgente legislazione italiana, non contempla una figura unitaria e standardizzata, ma prevede una sorta di *continuum*, capace di accogliere un ventaglio indefinito di tipologie. Al vertice *la firma elettronica avanzata* basata su un *certificato qualificato* rilasciato da un *certificatore accreditato* e creata mediante un dispositivo per la creazione di una *firma sicura*: corrisponde sostanzialmente alla firma digitale italiana. Al di sotto, la direttiva dà spazio a qualunque figura di firma elettronica, di cui dà la seguente definizione: *"dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione"*. Descrizione oltremodo vaga, che abbraccia anche tecnologie dai contenuti di sicurezza molto limitati, come il già descritto SSL, ma anche accorgimenti totalmente privi di qualunque connotato di sicurezza: persino una semplice immagine scannerizzata della firma autografa, che chiunque può procurarsi con straordinaria facilità.
L'evoluzione è in qualche modo fisiologica. La legislazione italiana del 1997, tra le primissime in Europa, si poneva l'obiettivo di rendere quanto più accettabile possibile la dirompente novità del

---

riferiscono ai cosiddetti *brutal attacks*, attacchi "stupidi", portati cioè provando in sequenza tutte le combinazioni possibili. Nel mondo reale, però, le minacce sono più sofisticate, e fanno ad esempio leva su sagaci accorgimenti che sfruttano errori di concezione dei softwares. SSL non fa eccezione: una sua vecchia edizione venne messa alla berlina nel 1996 da due studenti di Berkeley, Ian Goldberg e David Wagner; il loro lavoro, *Randomness and the Netscape Browser*, è accessibile alla pagina http://www.ddj.com/documents/s=965/ddj9601h/9601h.htm

7 Per una contrapposizione tra *Formalistic model* e *Risk-Based Model*, cfr Ford e Baum, *op. cit.*, p. 67.

8 Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (*Gazzetta Ufficiale delle Comunità europee* n. L 013 del 19 gennaio 2000 pagg. 12 - 20).

documento *paperless* a validità giuridica: a tal fine l'ovvia strategia era circondarsi dei migliori accorgimenti di sicurezza disponibili. Si aggiunga poi che le tecnologie digitali erano viste innanzitutto come uno strumento per lo snellimento della Pubblica Amministrazione: questo è un settore dove non si possono fare troppi sconti sul piano della certezza documentale e, nel contempo, occorre pure vincere resistenze e conservatorismi d'ogni specie, più o meno interessati. Tutto cospirava quindi verso un approccio estremamente prudente. La direttiva si muove invece a più ampio spettro. Da un lato non disconosce le peculiari esigenze legate all'uso della firma digitale in campo pubblico, sancendo anzi il diritto degli Stati di adottare a tal proposito tutti gli accorgimenti che loro paiano opportuni, purché *obiettivi, trasparenti, proporzionati e non discriminatori* (art. 3 Dir.). D'altro lato riconosce cittadinanza alle forme minori di firma elettronica richieste dalla pratica commerciale.
Queste ultime però non possono ovviamente che godere di uno *status* inferiore sotto il profilo probatorio. L'approccio della direttiva (art. 5), è liberale ma senza eccessi. La firma digitale possiede i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei, ed è ammessa come prova in giudizio. Ciò coincide tra l'altro con la previgente legislazione italiana e non pone speciali problemi. Per le firme elettroniche "minori" si è previsto invece quanto segue: *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.*

I Paesi dell'Unione sono quindi tenuti a non adottare normative che discriminino in via pregiudiziale (si noti l'avverbio *unicamente*) le firme elettroniche non provviste di specifici attributi di sicurezza, e sin qui non vi sarebbe granché da obiettare.

Il D.Lgs. 10/2002

Il fatto è che in sede di attuazione della direttiva il legislatore delegato italiano si è spinto molto più innanzi, senza che la direttiva lo richiedesse[9] né, quel che è peggio, che la legge delega lo autorizzasse: l'art. 6 comma 2 del D.Lgs 10/2002 così recita: *"Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare"*.
La firma elettronica, qualunque firma elettronica, è dunque sufficiente ad integrare gli estremi della forma scritta, salvo che sul piano probatorio il documento così sottoscritto è liberamente apprezzabile dal giudice. Sembra insomma che nel nostro ordinamento sia stata introdotta, quasi a contraltare della forma *ad probationem*, un'inedita forma *sine probatione*, che contraddice il comune insegnamento secondo cui la forma *ad substantiam* non è mezzo di prova[10], ma è anche

---

9 Al punto da far seriamente prendere in considerazione l'idea che la normativa italiana costituisca tout court violazione della direttiva europea.

10 Natalino Irti, *Il contratto tra faciendum e factum*, *Rassegna di diritto civile*, 1984, p. 938; anche in *Idola Libertatis*, Milano 1985, ed ora in *Studi sul formalismo negoziale*, Milano 1997, p. 120.

(e forse: soprattutto) predisposizione del mezzo di prova [11]. La situazione che così si viene a creare non è poi molto distante da quella che si riscontra tradizionalmente in caso di perdita o distruzione della scrittura, in cui il requisito sostanziale della forma è reputato storicamente soddisfatto, salve le incertezze sul piano probatorio. Constatare come il regime fisiologico di queste figure corrisponda a quanto sino ad oggi ha avuto cittadinanza nell'ordinamento solo come ipotesi patologica, sembra già commento sufficiente. Le applicazioni pratiche possono essere sconcertanti [12]: una firma elettronica intrinsecamente insicura potrà essere utilizzata per sottoscrivere (validamente!) una vendita immobiliare, salvo che il giudice potrà "liberamente valutare" l'attendibilità del documento.
Non minori perplessità desta il rinvio che il Decreto opera all'articolo 2214 c.c.: le scritture contabili possono essere regolarmente tenute avvalendosi di qualunque tipo di firma elettronica. Il problema è che le scritture contabili hanno funzione probatoria (art. 2709 c.c. ss.): resta alquanto misterioso come possano all'uopo essere state reputate idonee le firme elettroniche "minori", che la medesima legge (anzi: il medesimo comma) riconosce esser poco attendibili proprio sul piano probatorio.
La disposizione della legge d'attuazione che ha attirato le critiche maggiori è senza dubbio quella di cui all'articolo 6 comma 3: *"Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto"*. La prima ed ovvia reazione è stata individuare nella norma un'indebita equiparazione della firma digitale alla scrittura autenticata. Equiparazione formale che peraltro tutto è fuorché una novità, dato che era stata intravista dalla dottrina [13] già nell'imperio della previgente normativa. Questo non è però che l'inizio del problema.

---

11 Qualche rapido *click* del mouse sembra ancor meno idoneo a soddisfare l'altra tradizionale funzione attribuita alla forma, la responsabilizzazione del contraente. Ben altro discorso, anche qui, per la firma digitale propriamente detta: gli attuali *softwares*, pur non presentando la benché minima difficoltà di carattere informatico, hanno un'articolazione che conferisce al gesto della sottoscrizione un più che rispettabile grado di solennità.

12 Tra le prime e più vigorose critiche quelle di Manlio Cammarata e Enrico Maccarone, *A chi conviene la certificazione insicura?*, *Interlex*, 17 /01/02, http://www.interlex.it/docdigit/recepiment2.htm

13 Raimondo Zagami, *Firma digitale e sicurezza giuridica*, cit, p. 182, nel 2000 scriveva*: … in sostanza l'efficacia probatoria del documento informatico con firma digitale diviene in realtà diversa e superiore rispetto all'efficacia probatoria della scrittura privata cartacea come delineata all'articolo 2702cc, avvicinandosi piuttosto alla scrittura privata autenticata ex art. 2703cc*. Questione completamente diversa, naturalmente, è stabilire se la firma elettronica o digitale rappresenti una minaccia alla funzione notarile,

I problemi

Prendiamo a riferimento, in luogo della scrittura autenticata, il regime della scrittura privata semplice, come risultante dal combinato disposto dell'articolo 2702 c.c. e degli artt. 214 e 215 c.p.c.. In cosa differisce la nuova norma? Non nell'efficacia probatoria sino a querela di falso, che c'era già, quanto nella caduta del meccanismo del riconoscimento. Ma è concepibile un sistema di riconoscimento applicato alla firma digitale?

Una firma digitale non può dirsi neppure una firma (è solo una sequenza informe di *bytes*) se non è verificata sul piano informatico, se cioè non si accerta che la firma apposta è compatibile con la chiave pubblica del sottoscrivente. Compiuto con esito positivo tale test, si ha una ragionevole certezza che quella determinata firma è stata apposta utilizzando un determinato dispositivo di firma (*smart card* od altro). Si parla di ragionevole certezza, dacché la pretesa infrangibilità del segreto di chiave non è altro che un mito dal quale è opportuno sgombrare il campo con prontezza. Dal punto di vista puramente matematico, ricostruire il fattore ignoto partendo da quello noto (la chiave privata partendo da quella pubblica) non costituisce un'assoluta impossibilità, bensì una mera difficoltà di calcolo. La falsificazione della firma digitale (o meglio, la rivelazione del segreto di chiave) è quindi eventualità non del tutto da escludersi, soprattutto se si considera che eventuali falsificatori hanno a propria disposizione strumenti assai più efficaci del cosiddetto *brutal attack* 14.

Non solo: il dispositivo di firma può essere stato utilizzato da chiunque abbia ottenuto (col

---

ipotesi brillantemente demolita da Bernard Reynis, *Signature électronique et acte authentique: le devoir d'inventer* (relazione al XXII Congresso annuale del Comitato Francoitaliano del Notariato Ligure e Provenzale, Genova, settembre 2001, sul tema *Atti autentici in Europa e firma elettronica*) http://web.tiscali.it/conoge/italofrancese/ge.htm . Osserva Reynis che la funzione del notaro è ben altro che l'identificazione della parti: è garanzia di legalità, assistenza alle parti per il perseguimento dei loro obiettivi.

14 Vedasi a nota 6. Esistono inoltre tecniche crittografiche che possono semplificare il compito: se ad esempio si hanno a disposizione molti documenti sottoscritti con la medesima chiave, l'analista può valersi di una ricca base di dati su cui operare. Alcuni affermano persino che si possano ricavare dati utili misurando il tempo che i computers impiegano per le operazioni di firma. E' quindi certo che i migliori laboratori, come quelli dell'americana NSA, possono tentare qualcosa (*cosa* è ovviamente un segreto ben custodito), ma occorre essere realisti: chi fosse interessato a violare una chiave di firma, troverà in genere assai più semplice ed economico corrompere un collaboratore, od intercettare da un ambiente vicino gli impulsi elettromagnetici emessi dalla tastiera, onde scoprire il PIN della *smart card*

consenso del titolare, o con l'inganno o la violenza) il relativo PIN. A differenza di una perizia calligrafica, il test nulla ci dice quindi su chi abbia realmente maneggiato il dispositivo; detto in altri termini, sappiamo che la firma viene da quella *smart card*, ma non che sia stato davvero Tizio a firmare. Per questa ragione diversi studiosi [15] giustamente reputavano più corretta la definizione di sigillo, anziché firma, digitale. L'equivoco continua a mietere vittime, dato che la nuova norma discorre di "chi ha sottoscritto" un documento, soggetto a rigore ignoto.
Se trasportiamo queste ovvie considerazioni sul piano probatorio, la nebbia si fa fitta [16]. Non si può certo pretendere che chi intende valersi della firma provi che il congegno è stato davvero manovrato da Tizio: salvo casi eccezionalissimi, come potrebbe? Equivarrebbe in pratica ad azzerare il valore giuridico della firma digitale. Ogni altra strada conduce a far gravare su Tizio, su base oggettiva, il rischio di ogni uso improprio della *smart card* da lui fatta emettere. Anche laddove si riconoscessero a Tizio margini di prova contraria, questi risulterebbero infatti di interesse poco più che scolastico: neppure Tizio potrebbe verosimilmente dimostrare di non essere stato lui. Non si pensi alle ipotesi di smarrimento e sottrazione del dispositivo di firma, perché quelle sono coperte dalle apposite procedure di sospensione e revoca; l'uso di un certificato revocato o sospeso equivale ad una "non firma", e quindi il problema è azzerato alla radice.
Sotto questo limitato angolo visuale l'opzione del legislatore delegato, per quanto criticabile, appare a prima vista, se non altro, meno insensata: si spazza via un meccanismo che avrebbe avuto scarsa possibilità d'applicazione pratica, anche se, a rigore, una disfunzione del sistema informatico è sempre possibile.
Ci sono però altre fattispecie tutt'altro che teoriche che, per usare un eufemismo, pongono a dura prova il concetto di "piena prova sino a querela di falso". La più evidente è la morte del titolare. Può ben darsi che gli eredi ignorino l'esistenza di un certificato di firma elettronica intestato al defunto, e non segnalino quindi la circostanza al certificatore [17]. Laddove l'uso del dispositivo continui anche dopo la morte del titolare, le firme così apposte difetteranno probabilmente di un

---

prima di procedere alla sua sottrazione: avvalersi, insomma, delle "normali" tecniche di spionaggio industriale.

15 Silvia Miccoli, *La sicurezza giuridica nel commercio elettronico* (tesi di laurea), reperibile in Rete (formato Word) alla pagina http://web.tiscalinet.it/conoge/silmic.doc, seguita da **Danilo Giaquinto e Paola Ragozzo,** *Il sigillo informatico*, cit; vedasi anche Mario Miccoli, *Commercio telematico: una nuova realtà nel campo del diritto*, cit

16 Sul punto Mauro Orlandi, *L'imputazione dei testi informatici*, in *Rivista del Notariato*, 1998, p. 867 ss; Raimondo Zagami, *Firma digitale e sicurezza giuridica*, cit, p. 171 ss; Aurelio Gentili, *Documento informatico e tutela dell'affidamento*, in *Rivista di Diritto Civile,* 1998, II, p. 173.

17 Non a caso il legislatore del 1913, che evidentemente aveva un'idea un poco più precisa di quanto delicati siano i meccanismi per la produzione di documenti idonei a formare piena prova sino a querela di

qualsivoglia valore giuridico, ma di ciò i terzi non avranno modo alcuno di accorgersi, restando quindi indotti a fare pieno affidamento sui documenti in tal modo sottoscritti. Si può anche pensare di percorrere l'itinerario ricostruttivo opposto, magari ipotizzando che la rivelazione del PIN [18] da parte del defunto equivalga al conferimento di una forma peculiare di potere rappresentativo: in tale prospettiva potrebbe reputarsi applicabile l'articolo 1396 c.c., secondo comma, così salvaguardando la buona fede del terzo. Ad analogo esito si può forse pervenire facendo applicazione del principio dell'apparenza imputabile [19]. Ma questo è un classico esempio di coperta troppo corta: così ragionando si farebbe luogo ad una semplice operazione di *risk allocation*, trasferendo sugli eredi il rischio connesso ad usi abusivi *post mortem* del dispositivo di firma, ma senza realmente fare i conti con la sostanza della questione, che consiste nella possibile circolazione di firme assolutamente indistinguibili da quelle autentiche benché apposte dopo la morte del titolare.
Che il disconoscimento non continui ad essere uno strumento degno di considerazione anche con riferimento alla firma elettronica resta in sostanza da dimostrare.

Il ruolo dei certificatori

Il problema più serio è però, come suol dirsi, a monte: il ruolo esagerato che il sistema finisce con l'attribuire ai certificatori. La sicura attribuibilità di una firma ad un determinato soggetto evidentemente dipende, in radice, dall'accuratezza dell'identificazione compiuta in sede di rilascio del certificato. L'osservazione è banalissima, ma cionondimeno (o forse proprio per questo) stranamente trascurata [20]: la catena che unisce il titolare Tizio al documento firmato, che consente di imputare il documento a Tizio, si compone di due anelli: il test informatico che

---

falso, dettò l'articolo 38 della Legge Notarile, imponendo sia agli Ufficiali dello Stato Civile che agli eredi del notaro un obbligo di immediata comunicazione al Consiglio Notarile. La futura firma digitale del notaro certificata dal CNN verrà immediatamente revocata a cura del Presidente Distrettuale in occasione della cessazione dalle funzioni, qualunque ne sia la causa.

18 Qualora il defunto abbia portato il PIN con sé nella tomba, non si pone evidentemente problema alcuno, giacché il dispositivo di firma sarà inutilizzabile.

19 *Operante nel nostro ordinamento come principio di diritto effettivo*, scrive Cesare Massimo Bianca, *Commentario al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 670; sul punto, vedasi anche A.M. Gambino, *L'accordo telematico*, Milano, 1997, pag. 234 e segg.

20 E' curioso osservare come gli Autori meno a loro agio con la dimensione tecnologica del problema siano generalmente portati a compensare facendo sfoggio di un eccesso di zelo informatico, che finisce con l'obliterare proprio gli aspetti umani della questione.

permette di stabilire che una determinata firma è riferibile ad un determinato certificato, e l'identificazione fisica del richiedente compiuta al momento del rilascio del certificato stesso, in base alla quale si può affermare che fu Tizio, e non altri, a richiederne l'emissione. L'efficacia probatoria privilegiata sancita dalla nuova norma, avendo ad oggetto, *omisso medio*, l'associazione tra il titolare e la firma, copre per necessità logica ciascuna delle due fasi.
Anche tralasciando i rischi insiti nel primo passaggio, resta il fatto indubitabile che la fisica identificazione del richiedente non è diversa da quella compiuta in ogni altro contesto [21]. Tale funzione viene svolta in proprio dai certificatori oppure delegata dai certificatori alle *Registration Authorities*, soggetti esterni: società di servizi [22] ed agenzie di disbrigo pratiche, ad esempio, che agiscono tramite propri dipendenti. Istruttivi casi di falsificazione ai massimi livelli [23] si

---

21 Affidata cioè all'identificazione di una persona fisica eseguita da un'altra persona fisica. Lucio Valerio Moscarini, in *Commentario* (con Cesare Massimo Bianca ed altri) *al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 680/681, in più passaggi afferma che l'identificazione del soggetto è operata dal server, spingendosi sino ad affacciare l'ipotesi di "abuso perpetrato dal server" (*sic*), che a quanto ci consta appartiene non al diritto ma alla fantascienza.

22 Se ne trovano alcune tra le *Registration Authorities* che lavorano per Infocamere, ad esempio.

23 L'incidente più celebre ha visto come illustre protagonista VeriSign, società californiana leader mondiale del settore, che ha inavvertitamente rilasciato ad impostori due certificati intestati nientedimeno che a Microsoft, il 29 e 30 gennaio 2001 http://www.microsoft.com/technet/security/bulletin/MS01-017.asp Si trattava di due prestigiosi certificati *VeriSign Class Three*, destinati all'autenticazione dei programmi per computer. In concreto, avrebbero potuto essere utilizzati per inviare a qualunque utente di software Microsoft, ovunque nel mondo, sedicenti aggiornamenti di programmi esistenti, che il browser Microsoft Internet Explorer avrebbe espressamente garantito come provenienti da Microsoft stessa. Anche l'utente accorto avrebbe quindi proceduto senz'altro allo scaricamento, installando così nel proprio sistema qualunque tipo di programma (con funzione di spionaggio, ad esempio) al mittente fosse piaciuto. Si è appreso in quell'occasione che le due società statunitensi si affidavano per tale delicata funzione di certificazione a semplici conferme telefoniche, e che Microsoft Internet Explorer procedeva in automatico alla conferma della genuinità della firma senza previamente verificare se il certificato VeriSign non fosse stato eventualmente revocato.

rinvengono già nell'esperienza internazionale [24].
La norma introdotta dal legislatore delegato finisce dunque con l'equiparare questi soggetti ai pubblici ufficiali, atteso che l'unico strumento a disposizione resta la querela di falso. E questo pare davvero troppo [25]. Non si intende neppure entrare nella ben nota *querelle* su quale standard di accuratezza sia imposto al certificatore [26]. L'obiezione è più radicale: non si vede perché il titolare apparente del certificato debba obbligatoriamente far ricorso alla querela di falso per porre in discussione l'operato di un semplice soggetto privato, la cui attività (ai sensi dell'articolo 3 della direttiva, attuato con l'articolo 3 del D.Lgs. 10/2002) non è neppure sottoposta a previa autorizzazione od iscrizione ad un albo, ma a semplice "avviso".
Anche ammesso che questo snodo trovi soddisfacente sistemazione, resta comunque assodato

---

24 Nella prassi mondiale i diversi livelli di sicurezza non si limitano ai diversi tipi di firma elettronica (forte, debole) ma addirittura all'interno della cosiddetta firma forte (quella cioè a chiavi asimmetriche ed autorità di certificazione) vi sono – in funzione del corrispettivo pagato all'ente certificatore – diversi livelli di certezza nell'identificazione del titolare, il più basso dei quali non prevede alcun contatto fisico fra autenticatore e richiedente, ma il semplice controllo dell'esistenza dei dati del richiedente in altri *data base* (emittenti di carte di credito e simili), con le conseguenze, in fatto di certezza del diritto che non è difficile arguire. Sempre VeriSign offriva diverse classi di certificazione la più a buon mercato delle quali non prevedeva, appunto, alcun contatto fisico fra *Certification Authority* e richiedente, ma il semplice riscontro di dati offerti dallo stesso richiedente.

25 Del medesimo avviso Paolo Ricciuto, *La "nuova" efficacia probatoria della firma digitale*, *Interlex* 14/02/02, http://www.interlex.it/docdigit/ricchiu5.htm . Nessun problema per la futura firma digitale del CNN, ove l'identificazione è affidata al Presidente Distrettuale.

26 Gianluca Dalla Riva, *I mille problemi della firma digitale (2)*, *Interlex*, 31/1/02, http://www.interlex.it/docdigit/dallariva2.htm, benché l'espressione usata dal legislatore del T.U. (articolo 9 del DPR 10/11/1997 N. 513, ora articolo 28 DPR 28/12/2000 n. 445*)* a proposito dell'identificazione del certificatore, "*con certezza*", sembri suggerire il dovere di un'indagine assai più rigorosa di quella che si viene profilando sul mercato, per ovvie esigenze di costi. Si noti poi che tale obbligo di identificazione, dopo l'attuazione della Direttiva, continua a sussistere solo per le firme digitali e le altre firme basate su certificato qualificato (articolo 11 comma 3 D. Lgs. 10/2002; allegato II lettera d della Direttiva 93/1999),

che, laddove il certificato sia stato rilasciato correttamente e non revocato, al titolare sarà giuridicamente riferibile tutta l'attività a rilevanza giuridica posta in essere con tale dispositivo, anche qualora in concreto manovrato da terzi. In tale prospettiva, all'ipotesi di vera e propria consegna da parte del titolare è assimilato il caso dell'uso da parte del terzo tollerato dal titolare. L'uso consentito (o tollerato) da parte del titolare deve essere inquadrato nell'istituto della rappresentanza 27, sia pure con le distinzioni che occorre fare in ordine alla peculiarità del fatto che, contrariamente a quel che normalmente accade, non è la spendita del nome del rappresentato che può mancare, ma è l'identità del rappresentante che rimane ignota alla controparte. In ogni caso, in funzione del già ricordato principio dell'apparenza imputabile, dovrà trovare tutela il terzo che abbia riposto il proprio affidamento sull'apparente situazione, a preferenza del titolare che avendo trasferito il possesso della chiave al terzo, autorizzandone, o tollerandone, così l'uso, ha dato luogo all'apparente situazione per cui le dichiarazioni provenienti dal terzo utilizzatore appaiono all'esterno come se fossero genuinamente provenienti dallo stesso titolare.
Le *smart cards* recentemente rilasciate da Infocamere ai notai, ad esempio, possono essere utilizzate per firmare qualsivoglia documento, ivi compresa la vendita di un immobile appartenente al notaio stesso; il contratto così concluso, in base alla nuova normativa, formerà piena prova sino a querela di falso. Trattandosi di firma digitale propriamente detta, e non di una firma elettronica minore, non si può neppure fare affidamento sul filtro rappresentato dal libero apprezzamento del giudice. Non resta che la procellosa via della querela di falso 28, con difficoltà

---

mentre non è previsto per la firma elettronica semplice.

27 Il Tribunale di Cremona (sentenza 16 giugno 1998, in *Cassazione penale*, 1999, 995, con nota di Francesco Nuzzo) si è trovato a decidere in sede penale sul caso di un titolare di tessera Bancomat che aveva denunziato alcuni prelievi abusivi. Le videoregistrazioni eseguite dalla Banca consentirono di stabilire che il responsabile era il figlio del titolare, il quale aveva evidentemente potuto procurarsi il PIN in ambito familiare; il padre fece luogo a remissione della querela, senza con ciò impedire il giudizio trattandosi di reato perseguibile d'ufficio. Le peculiarità del caso e le specificità tecniche dell'ambito penalistico hanno ovviamente influito sui giudici cremonesi, ma è cionondimeno interessante che si dia soluzione favorevole all'imputato argomentando *dall'esistenza, già al momento dei fatti contestati, di un'autorizzazione - tacita, ma non per questo meno significativa - all'utilizzazione di tale tessera all'interno della famiglia*.

28 In diretta polemica con Raimondo Zagami, nega recisamente tale possibilità Salvatore Tondo, *Formalismo negoziale tra vecchie e nuove tecniche*, in *Rivista del Notariato*, 1999, p. 956, osservando che in simili casi si è dinanzi ad una firma vera. Col che si trascura forse il fatto che la querela di falso è per

probatorie ai limiti dell'insormontabile.
In questa direzione assumono uno speciale significato, forse finora un poco sottovalutato, le limitazioni all'uso che possono comparire nei certificati di firma. Anche i certificati CNN sono previsti con una speciale e ben mirata limitazione di tipo qualitativo, mentre quelli correnti non l'hanno. *Nihil sub sole novi*: anche il sistema Bancomat è sorretto dalle limitazioni di prelievo giornaliere. Se un bandito da strada, estorcendoci carta e PIN, potesse svuotare interamente tutti i nostri conti e dossiers titoli di qualunque banca, probabilmente nessuno avrebbe mai chiesto l'emissione di una tessera Bancomat.
In una prospettiva appena più lontana, occorrerà seriamente lavorare all'introduzione di sistemi di protezione biometrica, che impediscano l'uso del dispositivo di firma a persone diverse dal titolare. Benché le tecnologie siano disponibili e sperimentate, l'industrializzazione di siffatti prodotti non è ancora giunta ad uno stadio tale da rendere agevole la realizzazione di strutture su larga scala totalmente affidabili e standardizzate. Inoltre, quando l'introduzione delle tecniche di biometria si limitasse a sostituire il PIN, sì da consentire o negare, *tout court*, l'accesso al sistema, il problema del legame fisico fra titolare e sottoscrizione digitale del documento, continuerebbe a rimanere irrisolta: la vera equiparazione fra firma autografa e firma digitale avverrà soltanto quando i dati biometrici prelevati dal titolare al momento della sottoscrizione saranno computati nell'algoritmo di firma sì da garantire che la firma digitale sia stata apposta dal soggetto le cui caratteristiche fisiche corrispondono a quelle del titolare del dispositivo di firma.[29]

Comunque sia di ciò, la distanza tra il documento provvisto di firma digitale e l'atto notarile resterà, a quanto è dato vedere, un fossato incolmabile. L'indagine sulla capacità e legittimazione del sottoscrivente, la garanzia di un'adeguata informazione e riflessione intorno al contenuto dell'atto, la verifica della legalità del negozio e della sua idoneità a conseguire l'obiettivo desiderato, sono tutti elementi indispensabili per una larga gamma di operazioni, e sui quali la firma digitale, anche nelle visioni più futuristiche, nulla ha da dire.

---

giurisprudenza costante (da ultimo, Cass., sez. II, 12 giugno 2000, n. 7975) il rimedio per il caso di abusivo riempimento del biancosegno, fattispecie ove l'autenticità della firma non è in discussione. Ampiamente sul punto Mauro Orlandi, cit., p. 874. Nel senso dell'ammissibilità della querela di falso, con Zagami, la dottrina più autorevole, guidata da Cesare Massimo Bianca, *op. loc cit.*

29 La ricerca più avanzata in campo di firma digitale è appunto in tal senso: l'industria informatica Novell ha già in fase di sperimentazione sistemi del genere descritto.