PAOLO CONSALES

L'ABUSO DELLA FIRMA DIGITALE ED I RIMEDI ESPERIBILI

SOMMARIO: 1. Introduzione. — 2. Modalità concreta di falsificazione della firma digitale. — 3. Disconoscimento. — 4. Querela di falso.

1. Introduzione

L'articolo 10 terzo comma del D.P.R. 28 dicembre 2000 n. 445[1] riconosce al documento informatico sottoscritto con firma digitale il valore probatorio della scrittura privata, mediante il rinvio all'articolo 2702 cod. civ. La norma lascia aperti una serie di problemi: il primo e più importante è stabilire se il rinvio è fatto al solo articolo 2702, ovvero a tutto il sistema di norme che tale articolo presuppone. Si fa, in questo caso, riferimento non solo all'articolo 2703 cod. civ., ma, anche e soprattutto, agli articoli 214 ss. codice di procedura civile, in tema di disconoscimento e querela di falso.

Il problema, in altre parole, è verificare l'applicabilità delle disposizioni in materia di disconoscimento anche al documento informatico sottoscritto con firma digitale, cioè, in ultima istanza, controllare se anche la firma digitale possa essere disconosciuta e, conseguentemente, sottoposta alla procedura di verificazione ed alla successiva[2] querela di falso.

L'esigenza del disconoscimento e della procedura di verificazione si pone, in relazione alla sottoscrizione su supporto cartaceo, nei casi in cui un soggetto ritenga che la sottoscrizione apposta ad un documento presentato in giudizio non possa, nonostante l'apparenza, essere a lui imputata. Si pone cioè nel caso in cui ad un documento sia apposta, o si ritenga essere stata apposta, una sottoscrizione apocrifa. In questo caso il codice di procedura civile detta delle norme precise, in ordine ai tempi, agli oneri ed

[1] « Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa », pubblicato nella G.U. del 20 febbraio 2001 n. 42. Di seguito T.U.

[2] In ordine logico.

alle modalità che devono essere rispettate per potersi servire di questa procedura.

Tali ultime sono norme necessarie per identificare con certezza, almeno da un punto di vista processuale, il soggetto a cui un determinato documento può essere imputato, cioè il soggetto da cui proviene un determinata dichiarazione[3].

Lo strumento che permette di imputare un documento ad un soggetto, come sappiamo, è stato storicamente individuato nella sottoscrizione, di cui una delle funzioni tipiche è proprio quella di permettere non solo l'imputazione di un testo ad un soggetto[4], ma anche quella di fare in modo che lo stesso soggetto a cui il testo è imputato, ne assuma la paternità[5]. L'assunzione di paternità comporta, come risaputo, nel caso in cui il testo sia ad esempio un contratto, che il sottoscrittore è tenuto ad adempiere alle obbligazioni indicate nel contratto stesso. Così, per evitare che un soggetto sia obbligato ad adempiere ad obbligazioni che non ha mai contratto, sono previste la procedura di verificazione, consequenziale al disconoscimento[6], e la querela di falso.

Per quel che riguarda i documenti informatici tale strumento[7] è stato individuato nella firma digitale, che, grazie al sistema di crittografia a doppia chiave asimmetrica, è in grado di garantire non solo la segretezza e l'integrità del documento, ma anche la sua provenienza.

Ciò non esclude che per la firma digitale si possa porre un problema analogo a quello della sottoscrizione: è infatti possibile che la firma digitale sia apposta da un soggetto diverso rispetto al tito-

---

[3] È necessario precisare che il problema dell'identificazione si pone in maniera molto diversa a seconda che il destinatario della dichiarazione sia o meno presente nel momento in cui questa viene emessa. Se, ad esempio, Tizio afferma qualcosa alla presenza di Caio, oralmente o digitando sulla tastiera del suo computer, il problema di identificare il mettente della dichiarazione non si pone, in quanto questa è stata resa alla presenza del destinatario. Diversamente avviene se la dichiarazione è resa in assenza del soggetto cui è diretta: affinché possa essere, non solo considerata come dichiarazione, ma anche imputata al soggetto che la ha emessa, è necessario che il destinatario sia messo in condizione di conoscerne il mittente tramite uno strumento diverso dalla percezione diretta.

[4] Funzione cosiddetta indicativa. Con tale funzione si intende che il documento sottoscritto indica, se riconosciuto o legalmente considerato come riconosciuto (fino a querela di falso), l'autore del documento, ossia la corrispondenza tra il segno grafico e la persona che lo ha apposto. La sottoscrizione è, cioè, necessaria affinché il documento privato possa essere giuridicamente imputato a chi ne viene indicato come autore, in quanto, non avendo i privati il potere di attribuire alle loro dichiarazioni il carattere di veridicità, occorre accertare la riferibilità soggettiva e l'imputabilità giuridica del documento in cui tali dichiarazioni sono oggettivate al fine di individuarne l'autore.

[5] Funzione cosiddetta dichiarativa. Tale funzione attiene invece all'assunzione di paternità di quanto è rappresentato nel documento sottoscritto dal soggetto. Il documento, infatti, potrebbe essere stato redatto da altri ed è la firma che ne permette la riconducibilità ad un dato soggetto che assume il contenuto di detto scritto come espressione della sua personalità e volontà.

[6] Per ulteriori precisazioni vedi *infra* nel testo.

[7] Lo strumento che permette l'imputazione ad un soggetto di un documento informatico.

lare della chiave privata collegata a quella pubblica certificata. Il sistema di crittografia asimmetrica a doppia chiave[8] non garantisce un grado di sicurezza assoluto, per cui certamente non è da escludere la possibilità di una firma digitale apocrifa, cioè una firma riconducibile (attraverso la verifica con un valido certificato) ad una certa persona, ma da questa non realmente apposta. L'apocrifia della firma digitale può derivare o da una certificazione non veritiera, ovvero, in particolare per il caso che si cerca di esaminare in questo scritto, dall'uso abusivo della chiave privata da parte di persona diversa dal titolare. In quest'ultimo caso è stato evidenziato[9] che l'uso della chiave privata di sottoscrizione da parte di persona diversa dal titolare, può derivare dall'uso del dispositivo di firma[10] in cui essa è contenuta, ovvero, sebbene questa, per ragioni tecniche, sia un'ipotesi più difficile da realizzarsi in concreto, dall'uso diretto della chiave stessa (nella sua forma di codice informatico). Per limitare questo rischio il D.P.C.M. 8 febbraio 1999[11] disciplina la generazione delle chiavi di sottoscrizione (articoli 5, 6, 7), la loro conservazione (articolo 9), la generazione e verifica delle firme[12]. La ricostruzione della

[8] Tale sistema è alla base del funzionamento della firma digitale.

[9] ZAGAMI, *Firma digitale, e sicurezza giuridica*. Cedam, 2000, pag. 268.

[10] In ordine al dispositivo di firma ed alle modalità pratiche di funzionamento della firma digitale vedi *infra* nel testo.

[11] Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999. « Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3 del D.P.R. 10 novembre 1997, n. 513. Di seguito D.P.C.M.

[12] Articolo 5: Generazione delle chiavi.

« 1) La generazione della coppa di chiavi deve essere effettuata mediante apparati e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.

2) Il sistema di generazione delle chiavi deve comunque assicurare:

a) la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;

b) l'equiprobabilità di generazione di tutte le coppie possibili;

c) l'identificazione del soggetto che attiva la procedura di generazione.

3) La rispondenza dei dispositivi di generazione delle chiavi ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC o superiori ».

Articolo 6: Modalità di generazione delle chiavi

« 1) La generazione delle chiavi di certificazione e marcatura temporale può essere effettuata esclusivamente dal responsabile del servizio che utilizzerà le chiavi.

2) Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.

3) La generazione delle chiavi di sottoscrizione effettuata autonomamente dal titolare deve avvenire all'interno del dispositivo di firma ».

Articolo 7: Generazione delle chiavi al di fuori del dispositivo di firma

« 1) Se la generazione delle chiavi avviene su un sistema diverso da quello destinato all'uso della chiave privata, il sistema di generazione deve assicurare:

a) l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura;

b) il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui verrà utilizzata.

2) Il sistema di generazione deve essere isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto contro i rischi di interferenze ed intercettazioni.

chiave, senza possedere il dispositivo di firma, è un'operazione di crittoanalisi, che può basarsi su un attacco analitico[13] oppure su un attacco esaustivo[14]. L'autore che si è occupato della questione[15] precisa anche che la sicurezza di una firma digitale deriva comunque da un approccio globale, per cui non servirebbe a nulla, ad esempio, un cifrario inattaccabile[16], se poi non si osservano delle ulteriori precauzioni, dato che un eventuale attacco verrebbe rivolto all'anello più debole della catena. Ad esempio, oggetto dell'attacco potrebbero essere le carte che costituiscono i dispositivi di firma, ovvero il sistema di generazione della firma ed altri elementi ancora. Tutto questo conferma che una sicurezza informatica assoluta, come gia accennato, è inconcepibile: donde

3) L'accesso al sistema deve essere controllato e ciascun utente preventivamente identificato. Ogni sessione di lavoro deve essere registrata nel giornale di controllo.

4) Prima della generazione di una nuova coppia di chiavi, l'intero sistema deve procedere alla verifica della propria configurazione, dell'autenticità ed integrità del software installato e dell'assenza di programmi non previsti dalla procedura.

5) La conformità al sistema ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC o superiori ».

Articolo 9: Formato della firma

« 1) Le firme generate secondo le regole contenute nel presente decreto debbono essere conformi a norme emanate da enti riconosciuti a livello nazionale od internazionale ovvero a specifiche pubbliche (Publicy Avilable Specification - PAS).

2) Alla firma digitale deve essere allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica ».

Articolo 10: Generazione e verifica delle firme

« 1) Gli strumenti e le procedure utilizzate per la generazione, l'apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, chiaramente e senza ambiguità, i dati a cui la firma si riferisce e richiedere conferma della volontà di generare la firma.

2) Il comma 1 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del sottoscrittore.

3) La generazione della firma deve avvenire all'interno di un dispositivo di firma così che non sia possibile l'intercettazione del valore della chiave privata utilizzata.

4) Prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all'identificazione del titolare.

5) La conformità degli strumenti utilizzati per la generazione delle firme ai requisiti di sicurezza imposti dal presente decreto deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC o superiori.

6) La conformità degli strumenti utilizzati per la verifica delle firme ai requisiti di sicurezza imposti dal presente decreto deve essere verificata secondo i criteri previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC o superiori ».

[13] L'attacco analitico si rivolge contro l'algoritmo di cifratura e da questo tenta di ottenere un metodo matematico per risalire alla chiave. Una volta che tale metodo è individuato, tutti i messaggi cifrati con quel certo algoritmo potranno essere facilmente decifrati. ZAGAMI, cit., pag. 269.

[14] L'attacco esaustivo al criptogramma consiste nel passare in rassegna sistematicamente tutte le possibili chiavi fino a quando non si trova quella giusta. Più lunga è la chiave, maggiore è la resistenza ad un attacco di questo tipo. Le difficoltà di provare tutte le possibili combinazioni infatti crescono in modo esponenziale con il numero di bits usati: l'aggiunta di un solo bit alla chiave, ad esempio, raddoppia il numero di chiavi possibili. Dall'altro lato, però, va ricordato che i tempi di ricerca delle chiavi si riducono man mano che aumenta la potenza dell'hardware. ZAGAMI, cit., pag. 269.

[15] ZAGAMI, cit., pag. 271.

[16] Per cifrario si intende il sistema tecnico (crittografia asimmetrica) che è alla base della firma digitale,

la possibilità, non solo teorica, di una firma digitale apocrifa; il che fa sorgere il problema, che verrà affrontato in questo articolo, dei mezzi processuali che l'ordinamento mette a disposizione del soggetto, il cui nome viene speso nelle relazioni giuridiche, per dimostrare l'apocrifia stessa. Altro problema, è, invece, quello di stabilire entro quali limiti il soggetto che risulta sottoscrittore apparente del documento possa essere vincolato al documento stesso. In altre parole si tratta di stabilire se, in base alle disposizioni del T.U. ed ai principi generali dell'ordinamento, il soggetto sarà comunque chiamato ad adempiere le eventuali obbligazioni contenute nel contratto sottoscritto con la sua firma digitale, ovvero se, in qualche modo, avrà la possibilità di opporre alla controparte, che ne richiede l'adempimento, l'apocrifia.

2. Modalità concreta di falsificazione della firma digitale

Prima di discutere dell'ammissibilità o meno del disconoscimento in relazione alla firma digitale si rende necessario spiegare, brevemente, quale sia il problema che realmente si pone, cioè come sia concretamente possibile apporre ad un documento informatico una firma digitale apocrifa, cioè una firma che appartiene ad un soggetto diverso rispetto al reale sottoscrittore[17].

Il legislatore ha previsto come meccanismo di firma il sistema delle smart card. Sono delle carte magnetiche al cui interno è contenuto un microprocessore in cui è memorizzata la chiave privata della firma digitale. Quest'ultima è, infatti, composta da un numero di bit talmente alto[18] da non poter essere ricordata a memoria, per cui la memorizzazione all'interno di un processore diviene indispensabile.

La lettura di queste smart card sarà effettuata tramite degli appositi componenti hardware, che, ovviamente, andranno installati sul proprio personal computer.

La smart card, per poter essere concretamente utilizzata, va inserita all'interno di questa componente hardware che procederà alla lettura. Per poter firmare un documento si rende necessario digitare un codice segreto[19], detto P.I.N.[20]: digitato il codice se-

[17] Va precisato che, seppure pensabile in teoria, la falsificazione della firma digitale nella pratica è di difficile realizzazione, in quanto la sua falsificabilità è di 1.500.000 volte più difficile della falsificabilità della firma autografa.

[18] Il D.P.C.M. ha infatti disposto che la lunghezza minima della chiave deve essere di 1024 bit.

[19] Questo ci permette di affermare con certezza che l'elemento che concretamente dovrà essere conservato con cura dal titolare della firma digitale non è tanto la chiave privata, come visto memorizzata nel processore interno alla smart card, quanto il codice segreto necessario per utilizzare la smart card.

[20] Personal Identification Number.

greto, il computer apporrà automaticamente la firma digitale al documento informatico.

È quindi possibile comprendere che, in realtà, quando si parla di firma digitale apocrifa si fa riferimento non tanto all'abuso della chiave privata, quanto all'utilizzazione abusiva del P.I.N. In altre parole si intende l'ipotesi in cui un soggetto riesce ad entrare in possesso non solo del meccanismo di firma altrui, la smart card, ma anche del relativo P.I.N.; tale soggetto, quindi, inserisce il dispositivo nell'apposita componente hardware, che provvede al suo riconoscimento; una volta riconosciuta la smart card e la chiave privata in essa contenuta, il software, necessario per il funzionamento della componente hardware di lettura della smart card, « chiede » che venga digitato il codice segreto. Se risulta esatto, il programma apporrà la firma digitale al documento informatico, imputandolo giuridicamente al legittimo titolare di quest'ultima, soggetto diverso rispetto al « reale » sottoscrittore[21][22].

3. Disconoscimento

Spiegato come concretamente si possa avere un abuso della firma digitale, si pone il problema, molto dibattuto in dottrina[23],

[21] Da un punto di vista pratico, il meccanismo è molto simile a quello utilizzato per il bancomat. Anche in questo ultimo caso si tratta di una carta con una banda magnetica che ha memorizzato determinate informazioni, per la cui utilizzazione è necessario inserirla in uno sportello abilitato e digitare il codice segreto. Va però precisato che da un punto di vista giuridico i problemi che si pongono, con le relative soluzioni, sono diverse.

[22] I problemi relativi all'abuso della firma digitale potrebbero essere superati nel momento in cui il codice segreto sarà determinato da una componente fisica irripetibile ed ovviamente non separabile dal titolare della chiave privata (quali potrebbero essere le impronte digitali, oppure l'occhio, ecc.). In altre parole si fa riferimento alla concreta attuazione delle chiavi biometriche. Da più parti in dottrina sono stati sollevati dubbi su tale tipo di chiave. Non solo si dubita circa la possibilità tecnica di realizzare un meccanismo hardware che garantisca una perfetta attuazione, ma ci sono autori che dubitano persino della loro sicurezza, affermando che comunque il problema dell'apocrifia della firma digitale non può essere superato semplicemente prevedendo un diverso tipo di chiave per il funzionamento della smart card. è stato precisato (Zagami, cit., pag. 65), che l'eventuale impiego di dati biometrici, quale strumento per l'accesso alla chiave privata, pur realizzando un elevato grado di sicurezza, non renderebbe, comunque, concettualmente « personale » o « somatica » la firma digitale, nel senso di come tale requisito si intende nella sottoscrizione. La firma digitale, infatti, non è direttamente collegata al dato biometrico, il quale costituisce solo il mezzo tecnico per accedere all'uso del dispositivo di firma dov'è contenuta la chiave privata occorrente per l'apposizione della firma. Ecco perché, in via di principio, non si possono escludere abusi.

[23] Vedi, tra gli altri, Delfini, *Il D.P.R. 513 e il contratto telematico* in *Contratti*, 1998, pagg. 293/305; Orlandi Francesca, *Il regolamento sul documento elettronico: profili ed effetti*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 1998, pagg. 743/772; Sarzana di Sant'Ippolito Fulvio, *Considerazioni in tema di documento informatico, firma digitale e regole tecniche. (Commento al D.P.C.M. 8-2-99)*, in *Corriere giuridico*, 1999, pagg. 799/809; Orlandi Mauro, *L'imputazione dei testi informatici*, in *Rivista notariato*, 1998, pagg. 867/877; Gentili Aurelio, *Documento informatico e tu-*

se la disciplina del disconoscimento possa applicarsi anche a quest'ultima. Ad esso non è possibile dare una soluzione certa, sia perché la dottrina è assolutamente divisa, sia perché il legislatore su questo argomento non si è mai espresso in maniera decisa, limitandosi, come noto, ad un rinvio all'articolo 2702 cod. civ., senza precisare se questo dovesse essere inteso come rinvio alla sola norma citata nell'articolo 10 del T.U., ovvero dovesse intendersi rinvio al complesso di norme che questa presuppone. D'altronde, come osservato da un autorevole dottrina[24], questi problemi sono conseguenza necessaria della logica di puro parallelismo, tra documento informatico e scrittura privata, seguita in questo campo dal legislatore. Ciò perché tale parallelismo subisce, dalla natura delle cose, alterazioni che fanno dubitare se veramente possa all'uno ed all'altro essere applicata la stessa disciplina.

A dimostrazione di quest'ultima affermazione sta il fatto che la dottrina è drasticamente divisa in ordine alla compatibilità della firma digitale con le caratteristiche del disconoscimento.

Compatibilità che non può essere valutata in assoluto, ma che va collegata al valore probatorio del documento informatico sottoscritto con firma digitale: l'articolo 10 T.U., nel determinarlo, rinvia, senza alcuna precisazione, all'articolo 2702 cod. civ.. Il rinvio crea qualche problema poiché tale ultima norma stabilisce infatti che la scrittura privata fa piena prova della provenienza delle dichiarazioni contro colui che l'ha sottoscritta; per ottenere tale risultato richiede il verificarsi di una delle seguenti condizioni: il riconoscimento della sottoscrizione da parte di colui che l'ha sottoscritta ai sensi dell'articolo 2702 cod. civ.; l'autentica da parte del notaio o da parte di un altro pubblico ufficiale a ciò autorizzato ai

tela dell'affidamento, in *Rivista di diritto civile*, 1998, pagg. 163/179; Moscarini Lucio Valerio, *Formalismo negoziale e documento informatico*, in *Studi in onore di Pietro Rescigno*, 1998, pagg. 1045/1069; De Santis, *Tipologia e diffusione del documento informatico. Pregresse difficoltà di un suo inquadramento normativo*, in *Corriere giuridico*, 1998, pagg. 383/396; Tripodi-Gasparini, *Firma digitale e documento informatico. Una disciplina unica per l'ambito pubblico e privato. Buffetti editore*, 1998; Bianca, *I contratti digitali* in *Studium Iuris 1998*, pagg. 1035/1040; Albertini, *Sul documento informatico e sulla firma digitale*, in *Giustizia civile*, 1998, pagg. 267/310; Piccoli-Zanolini, *Il documento informatico e la firma digitale*, in *I problemi giuridici di internet*, pagg. 57/104; Zagami, cit.; Sala, *La firma digitale. implicazioni e novità del nuovo strumento*, in *Archivio di diritto civile*, 1999, pagg. 681/685; Reggiani, *Forma e firma digitale: struttura e valore probatorio del documento informatico*, in *Documenti giustizia*, 1998, pagg. 1584/1600; Graziosi, *Premesse ad una teoria probatoria del documento informatico* in *Rivista trimestrale di diritto e procedura civile*, 1998, pagg. 481/529; Martino, *Nuovo regime giuridico del documento informatico. Franco Angeli*, 1998; Finocchiaro, *Documento informatico e firma digitale*, in *Contratto e impresa*, 1998, pagg. 956/987; Ferrari, *La nuova disciplina sul documento informatico* in *Rivista di diritto processuale*, 1999, pagg. 129/162; Fedeli, *Documento informatico e firma digitale: valore giuridico ed efficacia probatoria alla luce del Decreto del Presidente della Repubblica 513/1997* in *Rivista il diritto commerciale e del diritto generale delle obbligazioni*, 1998, pagg. 809/842.

[24] Gentili, cit., pag. 171.

sensi dell'articolo 2703 cod. civ.; il mancato disconoscimento tempestivo della parte contro cui è stata prodotta, ai sensi dell'articolo 215 numero 2 cod. proc. civ.; la contumacia della parte che l'ha sottoscritta, ai sensi dell'articolo 215 numero 1 codice procedura civile; l'esito positivo della procedura di verificazione esperita dalla parte producente il documento che sia stato tempestivamente disconosciuto ai sensi dell'articolo 216 codice procedura civile. In altre parole la sottoscrizione di per se stessa non è sufficiente a far conseguire l'efficacia di prova legale alla scrittura privata ai sensi dell'articolo 2702 cod. civ.; a tal fine è necessario il verificarsi di un determinato evento che, statuendo l'autenticità della sottoscrizione, attribuisca alla scrittura privata la speciale forza probatoria descritta dall'articolo 2702 cod. civ. In conclusione, il disconoscimento, espresso o tacito, l'autenticazione e la verificazione giudiziale rappresentano, alternativamente, un necessario elemento costitutivo della fattispecie disciplinata dall'articolo 2702 cod. civ., essendo la presenza di uno di questi elementi indispensabile al fine di poter valutare una scrittura privata come prova legale.

Il problema relativo al documento informatico è quello di stabilire se anche la scrittura privata informatica necessiti della ricorrenza di uno degli elementi appena descritti per avere il valore di prova legale, ovvero se essa, in ragione delle caratteristiche tecniche della firma digitale e di alcune indicazioni normative, possa produrre *tout court* l'efficacia di prova legale.

La dottrina, come già detto, è divisa su questo punto: chi ritiene[25] di dover applicare alla lettera le disposizioni del codice civile anche al documento informatico, reputando comunque necessario un riconoscimento della firma digitale, ammette la possibilità del disconoscimento; chi, diversamente, ritiene[26] che il documento informatico sottoscritto con firma digitale faccia piena prova fino a querela di falso esclude ovviamente il disconoscimento.

A sostegno della prima tesi si potrebbe affermare[27] che non è possibile escludere il disconoscimento, in quanto non ci sono appigli normativi per sostenerla: nel T.U. infatti non solo non c'è alcuna norma che autorizzi a pensare di poter considerare superfluo o inutile il disconoscimento, ma non c'è alcun riferimento normativo espresso al disconoscimento stesso ed alle conseguenze legali ad esso collegate. Questa mancanza andrebbe interpretata non nel senso di ritenere il disconoscimento escluso, bensì piuttosto,

[25] Vedi, tra gli altri, De Santis, cit., pag. 392; Ferrari, cit., pag. 145 ; Albertini, cit., pag. 288; Orlandi F., cit., pag. 750; Reggiani, cit., pag. 1594; Piccoli-Zanolini, cit., pag. 101.

[26] Vedi, tra gli altri, Finocchiaro, cit., pagg. 983 ss.; Graziosi, cit., pag. 515; Tripodi-Gasparini, cit., pagg. 39 ss.; Delfini, cit., pag. 295; Gentili, cit., pagg. 173 ss.; Bianca, cit., pag. 1037; Sala, cit., pag. 681.

[27] Reggiani, cit., pag. 1549.

al contrario, che nulla osti al suo permanere. Sarebbe infatti più ragionevole ritenere che l'eventuale esclusione di norme fondamentali come gli articoli 214, 215 codice procedura civile, fosse stata esplicita.

Si sostiene, inoltre, che la firma digitale non possa equivalere ad una sottoscrizione legalmente riconosciuta e che quindi, in difetto di riconoscimento, espresso o tacito, o di autenticazione possa essere disconosciuta e fatta, successivamente, oggetto di verificazione. Un autore[28] sottolinea che sarebbe impensabile far assurgere il documento informatico sottoscritto con firma digitale al ruolo di scrittura privata autenticata, rendendo superflua la necessità di ulteriori controlli, quasi che il titolare della firma digitale sia munito di un'autentica permanente. Sarebbe impensabile perché le norme della legge notarile potrebbero anche essere interpretate nel senso di assegnare al pubblico ufficiale, tramite il potere di autentica, il compito di garantire, non solo la legittimazione delle parti, ma anche che il negozio sia, nel suo complesso, coerente con l'ordinamento[29]. Modificando lo strumento tecnico negoziale[30], non per questo viene meno la funzione dell'autentica, che rimane in tutta la sua importanza giuridica e sociale. Di questo sembra prendere atto il legislatore, emanando l'articolo 24 T.U.[31]: la norma prevede l'autenticazione, da parte di un notaio o di un pubblico ufficiale autorizzato, della firma digitale. L'autenticazione consiste nell'attestazione che essa è stata apposta in loro presenza dal titolare, previo accertamento della sua identità perso-

[28] PICCOLI-ZANOLINI, cit.

[29] Va precisato che il testo normativo non è così esplicito e non consente un'interpretazione univoca in tal senso.

[30] Si intende in questo caso sostituendo il supporto cartaceo con il supporto informatico, e la sottoscrizione manuale con la firma digitale.

[31] Articolo 24: Firma digitale autenticata

« 1) Si ha per riconosciuta ai sensi dell'articolo 2703 del cod. civ., la firma digitale la cui apposizione è autenticata da un notaio o da altro pubblico ufficiale autorizzato.

2) L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, numero 1, della 16 febbraio 1913, n. 89

3) L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

4) Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizione dell'articolo 20 comma 3.

5) Ai fini e per gli effetti della presentazione di istanze agli organi della pubblica amministrazione si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.

6) La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposta la firma digitale e la validazione temporale a norma del presente testo unico ».

nale e della validità della chiave utilizzata. Ma la norma rende obbligatorio anche un controllo ulteriore, raggiungendo un risultato che la migliore dottrina notarile aveva gia realizzato: controllo ulteriore che consiste, da un lato, nel verificare la rispondenza del documento sottoscritto alla volontà della parte, dall'altro, nel certificare la sua non contrarietà al disposto dell'articolo 28 primo comma n. 1 legge 1913/89. Con riferimento a questi ultimi due controlli va però fatta una precisazione. Mentre la dottrina sembra concorde nell'applicabilità anche all'autenticazione di scritture private dell'articolo 28 legge notarile e soprattutto del relativo numero 1, molti dubbi vi sono circa l'applicabilità del controllo relativo alla rispondenza della scrittura privata alla volontà effettiva delle parti, fermo restando che alla scrittura privata non può essere applicato il penetrante controllo previsto per l'atto pubblico. A parte questi ultimi dubbi, si sostiene che la presenza dell'articolo 24 T.U. dimostri inequivocabilmente che la firma digitale va riconosciuta o comunque autenticata per assegnare alla scrittura privata il valore di prova legale; mancando quindi l'autenticazione, la firma digitale non è idonea ad assegnare valore legale alla scrittura privata e potrà essere disconosciuta e sottoposta alla procedura di verificazione.

Ad ulteriore sostegno di questa tesi, favorevole all'applicabilità del disconoscimento anche alla firma digitale, si afferma[32] che l'onere di disconoscere la firma digitale, onde evitare, ai sensi dell'articolo 215 numero 2 cod. proc. civ., che questa si ritenga legalmente riconosciuta, sia giustificato proprio dal fatto che la procedura di certificazione non garantisce, come gia sottolineato[33], contro l'apocrifia della firma. In altre parole si ritiene[34] necessario il disconoscimento in quanto è forte il rischio di frodi originato dall'uso improprio di chiavi asimmetriche.

Altre motivazioni potrebbero essere alla base dell'applicabilità in via analogica degli articoli 214 ss. codice procedura civile al documento informatico argomentando[35] che la *ratio* della verificazione sta nella minor forza di convincimento della scrittura privata rispetto alle altre prove liberamente valutabili, derivante a sua volta dal fatto che essa è privatamente precostituita[36] al pro-

---

[32] FEDELI, cit., pagg. 824-825.
[33] Vedi *ante* nel testo.
[34] FEDELI, cit., pagg. 824-825.
[35] DE SANTIS, cit., pag. 393.
[36] *Contra*: GRAZIOSI, cit., pag. 510. Tale autore ritiene che il documento informatico sottoscritto con firma digitale non possa essere qualificato come prova costituita, ma più giustamente va considerato come prova costituenda, cioè prova che si forma all'interno del processo. Tale autore sostiene infatti che, se anche è vero che la prova è materialmente costituita da un oggetto preesistente al processo (il supporto informatico su cui è memorizzata la dichiarazione e la firma digitale), non è meno vero che l'effetto rappresentativo si forma solo nel processo, quando cioè il giudice provvede ad accertare la corrispondenza tra le chiavi pubblica e privata. Si verrebbe così a creare una situazione che potrebbe apparire singolare: nel documento informatico la prova della dichiarazione in esso contenuta sarebbe documentale e

cesso. Tale autore ritiene che l'estensibilità potrebbe inoltre essere argomentata con un'ulteriore motivazione di carattere processuale. Se, infatti, si concepisse la verificazione come ulteriore strumento difensivo concesso alla parte che ha prodotto in giudizio un documento poi disconosciuto, l'identità di *ratio*, che consente l'applicazione analogica delle norme in questione, sarebbe, in questa prospettiva, rappresentata dalla mera compatibilità tecnica del meccanismo processuale in rapporto all'intenzione di assicurare un ulteriore corso ad ogni documento prodotto, non assistito dalla pubblica fede, disconosciuto, e verificabile.

Una volta accettata la possibilità del disconoscimento, tale corrente di dottrina si pone il successivo, in ordine logico, problema di verificare se i principi e le norme in tema di disconoscimento della scrittura privata su supporto cartaceo possano essere applicate *tout court* anche al documento informatico, ovvero la diversità del supporto rende necessarie delle modifiche applicative. In particolare, sono state proposte diverse soluzioni che ruotano attorno alla diversità del *thema probandum* dell'eventuale procedura di verificazione consequenziale al disconoscimento.

In via meramente accademica si potrebbe sostenere che le disposizioni in tema di disconoscimento possano, *sic et simpliciter*, essere applicate al documento informatico sottoscritto con firma digitale: cioè il soggetto contro cui è prodotto in giudizio il documento avrebbe soltanto l'onere di disconoscerlo tempestivamente, gravando sull'altra parte, cioè sulla parte che ha prodotto il documento in giudizio, dimostrare che sia stato proprio colui cui la firma è imputata, ad apporla materialmente. Lampanti sono le motivazioni che portano a bocciare questa impostazione: non solo si permetterebbe al titolare della firma digitale di invocare l'abuso senza provarlo[37], ma soprattutto si finirebbe per onerare la controparte di una prova meramente negativa dell'insussistenza di abusi o di illeciti da parte di terzi: sostanzialmente si tratterebbe di una cosiddetta *probatio diabolica*, ovviamente impossibile a realizzarsi. Non potendosi far ricorso alle scritture di comparazione, i mezzi istruttori per fornire tale prova sarebbero veramente ridotti al minimo, per non dire inesistenti. La prova, quindi, sarebbe certamente contraria ai principi processuali in tema di onere della prova.

Una parte della dottrina sostiene invece la tesi[38] secondo cui, per superare il disconoscimento, sia sufficiente la verificazione tecnica della firma digitale, ovvero sia la corrispondenza tra

quindi costituirebbe una prova costituita, mentre la prova della sua provenienza, ossia la prova dell'atto di assunzione di paternità, sarebbe costituenda.

[37] GENTILI, cit., pag. 173.

[38] Tra gli altri, ORLANDI M., cit., pag. 871.

chiave pubblica e chiave privata, senza permettere al presunto soggetto firmatario di dimostrare il contrario nella stessa sede del giudizio di verificazione. A sostegno di questa tesi, è stato affermato[39] che in questo caso non si precluderebbe il disconoscimento, pur rendendo particolarmente difficile il ripudio della paternità. Ulteriormente si afferma[40] che, una volta provata l'esistenza di un valido certificato, questo non solo sia opponibile in giudizio, ma costituisca anche il nesso di imputazione formale tra chiave e suo titolare. La stessa autrice ritiene necessaria questa modifica dei mezzi di prova per garantire l'applicabilità della disciplina del disconoscimento anche al documento informatico, in quanto il mancato adeguamento della disciplina processualistica al nuovo mezzo informatico inficerebbe, nella sua portata, la riforma. Questa tesi non è molto apprezzata neanche dagli autori che ritengono ammissibile il disconoscimento della firma digitale[41]: si afferma infatti che in questo caso il disconoscimento e la successiva verificazione perderebbero sostanziale significato, riducendosi ad una verifica tecnica della firma: operazione matematica che, si potrebbe aggiungere, andrebbe comunque fatta, indipendentemente dall'esplicito disconoscimento della firma stessa.

La tesi più accreditata, tra coloro che sostengono la compatibilità tra firma digitale e disconoscimento, è quella che tende ad ampliare il più possibile il *thema probandum* del giudizio di verificazione. La corrente di dottrina a sostegno di tale ipotesi[42] ritiene sia necessario che, a seguito della verifica tecnica della firma digitale, (verifica della corrispondenza tra chiave privata e chiave pubblica e dell'esistenza di un valido certificato), cioè dopo aver validamente e correttamente decifrato la firma digitale ed il documento a cui era apposta, il soggetto che risulta titolare della chiave privata utilizzata per sottoscrivere il negozio ha il difficile onere di dimostrare eventualmente di non essere il reale autore della firma. Si avrebbe, in sostanza un'inversione dell'onere della prova: non è più il soggetto che presenta il documento in giudizio a dover dimostrare che la sottoscrizione non è apocrifa, ma è il titolare della firma digitale a dover dimostrare l'esistenza di un abuso della sua chiave privata. Tale inversione dell'onere della prova è reso necessario non solo dal differente mezzo tecnico ma anche e soprattutto dalla presunzione di riferibilità della firma digitale ad un soggetto, che sorge a seguito della certificazione[43]. È possibile muovere una prima critica a tale tesi, che sarà poi decisiva nelle successive considerazioni in tema di disconoscimento della firma

---

[39] ORLANDI, cit., pag. 871.
[40] FEDELI, cit., pagg. 824-825.
[41] ZAGAMI, cit., pag. 176
[42] Tra gli altri vedi REGGIANI, cit., pag. 1594; ZAGAMI, cit., pag. 176; ORLANDI F., cit., pag. 750; FEDELI, cit., pagg. 824-825.
[43] Sulla presunzione di riferibilità vedi più diffusamente *infra* nel testo.

digitale: adottando questa impostazione si amplia troppo l'oggetto del giudizio di verificazione il quale, da un lato sconfinerebbe nell'ambito della querela di falso, certamente applicabile al documento informatico, rendendola praticamente superflua; dall'altro lato, eccederebbe anche l'ambito del disconoscimento e del giudizio di verificazione stesso, il cui scopo tradizionalmente non è quello di dimostrare un falso, quale si profilerebbe un abuso della chiave privata, ma quello di poter imputare una sottoscrizione ad un determinato soggetto, o meglio quello di dimostrare la negazione della riferibilità della firma all'apparente sottoscrittore, attraverso la denuncia della contraffazione della firma autografa.

L'ipotesi della disconoscibilità della firma digitale, come già accennato, non è condivisa da una parte consistente della dottrina che ritiene il disconoscimento e la successiva procedura di verificazione, incompatibili con il sistema della firma digitale, sia da un punto di vista tecnico, sia da un punto di vista normativo.

In primo luogo viene contestato il ragionamento secondo cui la mancanza di un richiamo normativo al disconoscimento non possa escluderlo; l'autore che si è occupato della questione[44], ritiene infatti che il richiamo effettuato dall'articolo 10 T.U. all'articolo 2702 cod. civ. vada riferito soltanto al tipo di efficacia probatoria previsto da questa norma, e non alla sua fattispecie astratta, ritenendo, oltretutto, che se il legislatore avesse voluto richiamare l'intera disciplina dell'articolo 2702 avrebbe utilizzato formule diverse, certamente più esplicite[45].

Elemento fondamentale per argomentare l'esclusione del disconoscimento della firma digitale viene individuato nella differente modalità con cui si stabilisce la paternità di un documento, rispettivamente attraverso la firma digitale e la sottoscrizione manuale. L'apposizione della firma digitale, come gia notato[46], non è, differentemente dalla sottoscrizione manuale, un atto intimamente connesso con la persona del dichiarante; è un atto che stabilisce una semplice relazione artificiale ed oggettiva tra chiavi asimmetriche e titolare della firma digitale. Questa relazione, a differenza di quanto avviene con la relazione di tipo soggettivo che si instaura tra sottoscrittore e sottoscrizione autografa, non è in grado di identificare l'effettivo autore di una determinata firma digitale facendo leva sulla personalità grafica del segno, bensì è in grado soltanto di stabilire che una determinata firma digitale proviene da una determinata chiave privata che è attribuita, in via esclusiva,

[44] GRAZIOSI, cit., pag. 515.

[45] GRAZIOSI, cit., pag. 515, ritiene che l'articolo sarebbe potuto essere così formulato: « Nei casi previsti dall'articolo 2702 il documento informatico sottoscritto con firma digitale fa piena prova fino a querela di falso… » oppure « Il documento informatico fa piena prova fino a querela di falso quando ricorre una delle condizioni di cui all'articolo 2702… »

[46] Vedi BIANCA, cit., pag. 1037.

ad un determinato soggetto. In altre parole, il differente tipo di rapporto che intercorre tra firma digitale e suo titolare non concederebbe, a differenza di quanto avviene per la sottoscrizione autografa, la possibilità, per il titolare della chiave, di affermare che quella firma non provenga da lui. Se verificata con esito positivo, la firma digitale unisce con certezza matematica[47] il titolare della chiave alla firma, non lasciando alcuno spazio per la sussistenza, almeno da un punto di vista logico, al disconoscimento. Più precisamente viene affermato[48] che « la firma digitale è intrinsecamente incapace di restituire la prova della paternità materiale, giacché rappresenta non l'autore della digitazione, bensì il titolare della chiave ». Tale tesi è sostenuta anche da elementi di carattere normativo, oltre che da quelli logici appena esposti. In primo luogo si fa riferimento alla presunzione di riferibilità della firma digitale al titolare del certificato che si ottiene a seguito della procedura di certificazione effettuata al momento della generazione ed assegnazione delle chiavi. Un autore[49] ritiene che, in tanto potrebbero sorgere dubbi sulla paternità di un documento cifrato con il sistema delle due chiavi asimmetriche, in quanto non sia stato previsto un sistema pubblico di certificazione delle chiavi. Tale mancanza, infatti, non darebbe alcuna garanzia sul fatto che l'autore ed il mittente corrispondano al soggetto titolare delle chiavi pubbliche impiegate, rendendo certamente ammissibile il disconoscimento. Ma la procedura di certificazione prevista dall'articolo 27 T.U.[50], nel garantire la corrispondenza tra un soggetto, la

[47] In realtà va precisato che una certezza matematica non può esistere perché questa si ritiene scientificamente impossibile. Il termine « matematica » è stato utilizzato in senso atecnico, come rafforzativo a fini di forma.

[48] ORLANDI, cit., pag. 870.

[49] TRIPODI-GASPARINI, cit., pagg. 38/40.

[50] Articolo 27 T.U.: Certificazione delle chiavi

« 1) Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 8 comma 1 deve munirsi di un'idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione,

2) Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro validità, sono consultabili in via telematica.

3) Salvo quanto previsto dall'articolo 29, le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto e tenuto aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 8 comma 2:

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

b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzione di amministrazione, direzione e controllo presso banche;

c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore ed il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 8 comma 2;

d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

4) La procedura di certificazione di cui al comma 1 può essere svolta anche da un

sua chiave pubblica e quella privata segreta, rende, per così dire, « autentica » la firma digitale una volta per tutte, fino alla scadenza del periodo di validità del certificato. Ecco il primo elemento che permette la ricostruzione della presunzione di riferibilità sopra accennata.

Rafforza tale ricostruzione l'articolo 28 secondo comma lett. *a*)[51]: nell'indicare analiticamente quali siano gli obblighi del certificatore, il legislatore, come prima incombenza, gli ha imposto di identificare « con certezza » la persona che fa richiesta di certificazione; ciò per rafforzare ulteriormente l'importanza della reale identità del soggetto ai fini della relazione oggettiva che si instaura con la chiave privata ad esso attribuito. Non si capirebbe altrimenti perché il legislatore abbia posto particolare attenzione all'esigenza di un'identificazione certa del richiedente e futuro titolare della firma digitale.

Ulteriori elementi normativi di sostegno potrebbero essere individuati nella disposizione definitoria dell'articolo 22 T.U. ed in particolare nella lettera *d*), che definisce la chiave pubblica. Si può ritenere che tale norma specifichi la funzione assolta dalla chiave pubblica, che consiste non solo, nell'accertare la validità della firma digitale, ma, utilizzando la chiave pubblica insieme al sistema di validazione[52], permette, contemporaneamente, di individuare chi ha apposto quella singola firma digitale. Il perseguimento di tale ultima finalità viene reso possibile, dal legislatore stesso, nel momento in cui indica, in maniera puntuale, il soggetto cui riferire la firma digitale verificata e valida. Esso non viene indicato dal legislatore in maniera generica, ma è individuato, all'articolo 22 lett. *d*) come il « titolare della (coppia di) chiavi asimmetriche », utilizzate per apporre e verificare la firma digitale. Di tale coppia di chiavi, come gia detto, quella privata è stata apposta per sottoscrivere il documento, e quella pubblica è utilizzata per verificarlo. Ponendo l'accento sul titolare della coppia di chiavi, il legislatore confermerebbe il legame oggettivo, e non soggettivo, che intercorre tra titolare e firma digitale; e la conseguenza sarebbe la presunzione, a questo punto da considerarsi assoluta, di riferibilità della firma digitale stessa al titolare della chiave privata; presunzione che permetterebbe così di escludere la compatibilità del disconoscimento con la disciplina del documento infor-

certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione Europea o dello Spazio Economico Europeo, sulla base di equivalenti requisiti.

[51] Articolo 9 secondo comma lett. *a*): Obblighi dell'utente e del certificatore.

« [...]

2) Il certificatore è tenuto a:

a) identificare con certezza la persona che fa richiesta della certificazione; [...] »

[52] Definito dall'articolo 22 lett. *a*):

« Ai fini del presente regolamento si intende [...]

b) per sistema di validazione il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità; [...] »

matico. Non potendo la firma digitale apposta alla scrittura privata informatica essere riferita ad altri se non al titolare delle chiavi, così come certificate, la firma deve considerarsi autenticata o, meglio, va qualificata come sottoscrizione considerata legalmente riconosciuta. In questo modo si potrebbe concludere che la scrittura privata informatica non avrebbe bisogno di alcuna delle condizioni, alle quali l'articolo 2702 cod. civ. fa riferimento, o rinvio, per vedersi assegnato il valore di prova legale della provenienza delle dichiarazioni; valore che, come anticipato, è proprio della scrittura privata riconosciuta, o considerata legalmente riconosciuta.

Un ostacolo a questa ricostruzione potrebbe essere individuato nell'articolo 24 T.U., che prevede la possibilità dell'autenticazione della firma digitale. Si potrebbe, in questo caso, argomentare che l'articolo 24, sulla base di questa ricostruzione, sarebbe superfluo, dal momento in cui la firma digitale di per sé può assegnare il valore di prova legale alla scrittura cui è apposta. È stato, però, prontamente ed autorevolmente sottolineato[53], che la possibilità dell'autenticazione della firma digitale non contrasta con la ricostruzione che tende ad escludere il disconoscimento della sottoscrizione digitale. L'articolo 24 T.U., infatti, non si limita a prevedere che la firma digitale, ai fini dell'autenticazione, sia apposta in presenza del notaio o del pubblico ufficiale autorizzato, da parte del titolare della chiave di cui abbiano precedentemente accertato l'identità e verificato la corrispondenza della chiave. La norma, come accennato[54], richiede due adempimenti ulteriori, che consistono nel verificare la corrispondenza della dichiarazione alla reale volontà del dichiarante e, sostanzialmente, la liceità, cioè la compatibilità con l'ordinamento giuridico, delle affermazioni contenute nel documento. L'autenticazione della firma digitale ai sensi dell'articolo 24 T.U., quindi, nonostante l'equiparazione fatta dal primo comma, assegna al documento informatico con essa sottoscritto un'efficacia diversa e tendenzialmente maggiore di quella risultante dall'autentica di una sottoscrizione manuale; efficacia che, permettendo di garantire la corrispondenza del documento alla volontà delle parti, nonché la sua liceità, assegna al documento informatico stesso un valore fideifacente più penetrante. Queste affermazioni permettono di superare anche l'ultimo ostacolo, rappresentato dall'articolo 24 T.U., alla corrente dottrinaria che esclude la compatibilità del disconoscimento con la firma digitale. Questa norma, infatti si armonizza perfettamente con il sistema da essi ipotizzato. La firma digitale infatti individua, con una sorta di evidenza pubblica, il soggetto da cui (si presume) provenga il documento, senza che sia necessaria un'autentica-

[53] GENTILI, cit., pag. 171.

[54] Vedi *ante* nel testo.

zione. Quest'ultima, invece, garantisce un *quid* in più, cioè che la chiave privata era ancora valida al momento della sottoscrizione, che la dichiarazione corrisponde alla reale volontà del soggetto interessato, che il contenuto del documento non è in contrasto con i principi dell'ordinamento.

In base alle motivazioni sopra esposte, pur comprendendo lo sforzo fatto dalla corrente della dottrina che ammette il disconoscimento della firma digitale al fine, non solo di garantire una maggiore aderenza al dettato normativo, quantomeno nella sua equiparazione tra firma digitale e sottoscrizione manuale, ma anche di conferire una maggiore certezza in ordine al reale sottoscrittore del documento informatico, non appare possibile non riconoscere fondate le motivazioni di ordine logico e normativo, che sono alla base della tesi esposta in fine. Sulla base di questa affermazione appare più corretto escludere la compatibilità tra disconoscimento e firma digitale. A tale conclusione si giunge anche per evitare che la procedura di verificazione, logicamente successiva al disconoscimento, possa ridursi o ad un controllo formale della corrispondenza tra le chiavi, pubblica e privata, ovvero finisca per sconfinare nel terreno che è proprio della querela di falso.

4. Querela di falso.

Considerato il disconoscimento, sia per questioni tecnico — logiche, sia per motivi di carattere normativo, incompatibile con la firma digitale, si pone ora il problema di verificarne la compatibilità con la querela di falso, altro strumento processuale che l'ordinamento mette a disposizione delle parti per provare la falsità di una scrittura[55]. Più precisamente, la querela di falso è l'unico strumento che l'ordinamento mette a disposizione per contestare le risultanze estrinseche dell'atto pubblico e della scrittura privata riconosciuta, autenticata o verificata, permettendo così di assegnarle il valore di piena prova legale senza alcuna ulteriore possibilità che questo venga rimesso in discussione.

Di questo istituto, da molto tempo, si è occupata la più autorevole dottrina[56]. Diversi i problemi che sono stati posti in evidenza ed ai quali sembra doveroso fare un accenno.

[55] In ordine alla querela di falso va ricordato che la più autorevole dottrina si è occupata della questione esaminando i vari aspetti di questo istituto giuridico.

[56] Vedi, tra gli altri, Denti, *Querela di falso*, in *Novissimo digesto italiano*, 1967, pagg. 664 ss.; De Stefano, *Falso (querela di falso) Voce* in *Enciclopedia del diritto*, Milano, 1967, pag. 696/718; Carnelutti, *Teoria del falso*, Padova, 1953; Saletti, *Affermazione di documenti e querela di falso*, in *Rivista di diritto processuale*, 1972, pag. 723/737; Saletti, *I limiti oggettivi della querela di falso: la scrittura privata non riconosciuta*, in *Rivista di diritto processuale*, 1973, pag. 558/568; Denti,

In primo luogo va ricordato che in questo caso si fa riferimento al falso in documenti, particolarmente in quei documenti che vengono prodotti in giudizio come elementi di prova e non ci si riferisce a qualsiasi tipo di falso, anche penale, quale potrebbe, ad esempio, essere il falso personale. Servendoci di questa premessa è possibile comprendere la definizione del falso del Carnelutti[57]: secondo tale autore il falso è il contrario del vero per cui è attributo non di un fatto, ma di un giudizio, il giudizio che si forma ricercando la verità del fatto rappresentato e del fatto della sua formazione e non il documento in quanto tale. Tale definizione sembra essere legata soprattutto alla considerazione che, intanto il documento riceve disciplina e tutela legale, in quanto sia connesso alla sua funzione di prova; ciò in quanto un fatto che serve a fornire una ragione e perciò a formare un giudizio è una prova e, di conseguenza, l'attributo di verità o falsità si trasferisce dai giudizi alle prove[58]. Una definizione ed una ricostruzione non condivisa da tutti[59]. Si sostiene infatti che spostando il connotato della falsità sul giudizio non si raggiungerebbe alcun risultato apprezzabile, mettendo per di più in ombra il fatto che il documento falso può essere rilevante anche fuori da un processo e dal suo valore probatorio: di ciò sarebbe conferma l'esistenza della querela di falso proponibile in via principale, affiancata alla querela di falso in via incidentale. I due tipi di querela hanno in comune la funzione, poiché entrambe sono dirette ad eliminare, mediante pronuncia giudiziale, il vincolo del giudice alla situazione probatoria legale risultante dal documento impugnato[60]. Diversa è invece la struttura, come è possibile comprendere esaminando, ad esempio, le modalità di proposizione. La querela principale va proposta mediante normale citazione e per essa non è necessaria alcuna autorizzazione, come differentemente previsto per quella incidentale, a sua volta proponibile mediante apposita dichiarazione ricevuta negli atti del processo pendente e, come già accennato, subordinata all'autorizzazione del giudice del processo nel quale è proposta.

Altra questione presa in esame è quella delle varie tipologie di falso[61]: è infatti possibile distinguere tra un falso materiale ed un falso ideologico; il primo incide sulla materialità del documento ed è a sua volta discernibile in falso per soppressione[62] [63], per con-

Querela di falso e scrittura privata non riconosciuta, in *Rivista di diritto civile*, 1956, pag. 594/598.

[57] CARNELUTTI, cit., pagg. 3 ss.

[58] CARNELUTTI, cit., pagg. 3 ss.

[59] DE STEFANO, cit., pagg. 698 ss.

[60] DE STEFANO, cit., pagg. 696 ss.

[61] Vedi, tra gli altri, CARNELUTTI, cit. pag. 20 ss.

[62] Intendendosi per soppressione l'eliminazione di una parte del documento.

[63] Secondo un autore (DE STEFANO, op. loc. ult. cit.), questo tipo di falso non potrà mai essere oggetto di una querela di falso, non sussistendo, per definizione, un documento contro il quale la querela possa rivolgersi. Sembra però possibile ipotizzare un'ipotesi di soppressione non dell'intero documento, ma di una parte di esso. In questo caso potrebbe essere intentata querela di falso, tramite la quale ricostruire le parti soppresse del documento.

traffazione[64], per alterazione[65 66 67]. Dal falso materiale va distinta l'ipotesi del documento che sia genuino ma non veritiero, cioè un documento nel quale non si ritrova alcuna manipolazione o deformazione, ma nel quale si registra una discordanza tra quanto dichiarato e quanto in realtà avvenuto. In questo caso siamo di fronte ad un falso ideologico[68 69].

Altro problema molto dibattuto è stato quello di stabilire se il giudizio sul falso sia un giudizio sul fatto o sul rapporto, in altre parole se sia un giudizio costitutivo o di accertamento. Quest'ultima non va considerata come una questione puramente accademica, in quanto la scelta dell'una o dell'altra soluzione inciderà anche sull'efficacia *erga omnes* della decisone del giudice in ordine alla falsità del documento[70]. Diverse sono state le argomentazioni portate a sostegno dell'una o dell'altra tesi, e sarebbe impossibile, oltre che fuori luogo in questa sede, riportarle tutte. Qui basterà ricordare che secondo una corrente di dottrina[71] il giudizio di

[64] In questo caso si tratta della formazione *ex novo* di una prova o di un documento atti a determinare un falso giudizio.

[65] Questo tipo di falso è considerato una figura intermedia tra la soppressione e la contraffazione, consistendo nell'eliminazione di una parte del documento e nella sua sostituzione con altra parte apocrifa.

[66] DE STEFANO, op. loc. ult. cit.

[67] In tutti questi casi ci si trova di fronte ad un documento non genuino.

[68] La dottrina (vedi, tra gli altri, CARNELUTTI, cit.; DE STEFANO, op. loc. ult. cit.) si è interrogata sulla differenza che intercorre tra falso ideologico e simulazione. Secondo il Carnelutti, il falso ideologico riguarda le dichiarazioni di verità e, quindi, i documenti narrativi; la simulazione, invece, riguarda le dichiarazioni di volontà e, quindi, i documenti dispositivi, quali i contratti o, più ampiamente, i negozi giuridici.

[69] La dottrina (vedi, ad esempio, MALINCONICO, *Cosiddetta falsità ideologica in scrittura privata e querela di falso*, in *Il nuovo diritto*, 1988, pagg. 179/184) e la giurisprudenza della cassazione (vedi, tra le altre, la sentenza 22 aprile 1987, o la sentenza 534/1978) hanno escluso la proponibilità della querela di falso per dimostrare la falsità ideologica della scrittura privata. Ciò in quanto il valore della scrittura privata, a differenza dell'atto pubblico, è limitato, ai sensi dell'articolo 2702 cod. civ., alla provenienza materiale delle dichiarazioni dal soggetto che l'abbia sottoscritta, e non comprende anche il contenuto del documento, liberamente valutabile dal giudice. Poiché la falsità ideologica incide sul contenuto del documento, ecco spiegato il motivo dell'inapplicabilità della querela di falso. Tale impostazione è sorretta anche da un altro elemento di carattere sistematico: l'articolo 2700 cod. civ. assegna all'atto pubblico il valore di piena prova non solo della provenienza e quindi dell'elemento materiale del documento, ma anche delle dichiarazioni delle parti e di tutto quanto sia avvenuto in presenza del pubblico ufficiale che ha redatto l'atto. Si dà, in altre parole, piena efficacia probatoria anche al contenuto del documento, giustificando così la querela anche contro il falso ideologico, possibile, in conclusione, contro l'atto pubblico perché giustificato da un solido appiglio legislativo.

[70] Secondo un autore (CARNELUTTI, cit.), il giudizio sulla falsità non può avere un valore *erga omnes* in quanto non esistono elementi tali da permettere una deroga al generale principio secondo cui la decisione di un giudizio civile ha efficacia solo tra le parti di quel giudizio. Né sarebbe possibile affermare il contrario basandosi sulla considerazione che la falsità di un documento, o, più in generale, di una prova non può non valere di fronte a tutti in quanto è un giudizio sulle qualità di questa e non sulla sua esistenza. Tale argomentazione è infatti considerata assolutamente superficiale, rilevando, tra l'altro, che non è escluso che un giudizio sul falso possa avere ad oggetto un rapporto.

[71] DI STEFANO, op. loc. ult. cit.; LIEBMAN, *L'oggetto del processo civile di falso*, in *Rivista trimestrale di diritto e procedura civile*, 1957, pag. 602/607. Tale ultimo autore sostiene la sua tesi ricordando che

falso avrebbe ad oggetto un fatto e non un rapporto, venendo così a costituire un giudizio di accertamento. Altra parte di dottrina[72] ritiene che oggetto del giudizio di falso sia una sorta di potere di annullamento, assegnando così al processo ed alla conseguente pronuncia giudiziale, un valore costitutivo. Va altresì ricordata l'opinione di coloro[73] che, partendo dall'identità del giudizio di falso civile in raffronto con quello penale e facendo riferimento ad una sorta di interesse pubblico alla eliminazione dei documenti falsi, riconoscono l'oggetto del giudizio di falso nel dovere del giudice di compiere questa eliminazione. Infine, un altro autore[74] ritiene che il legislatore abbia strutturato il processo come un giudizio dichiarativo della falsità o verità del documento e quindi come un anomalo giudizio di accertamento con funzione istruttoria, ossia con la funzione di garantire una posizione probatoria attuale o anche futura con efficacia *erga omnes*.

Accanto a questo problema relativo all'oggetto del falso, sembra opportuno prendere in considerazione anche la questione della portata della querela civile. In altre parole, si tratta di stabilire se l'accertamento riguardi solo il *quid falsi* o anche il *quid veri*. Un autore[75] ritiene che la decisione sul falso oltre ad individuare ciò che è falso, permette di stabilire quale sia il vero che il falso aveva coperto. Lo stesso autore precisa altresì che, in relazione ai diversi tipi di falso materiale, non ogni alterazione, anche accidentale del documento è sufficiente a fondare una querela di falso, dovendo il proponente allegare e dimostrare la diversità del testo esistente rispetto a quello originario. Da questa diversità si potranno trarre gli elementi necessari per ricostruire il documento nel suo testo genuino.

Per quel che riguarda la legittimazione attiva e passiva, non sembrano esserci particolari problemi in caso di querela incidentale: in quest'ipotesi legittimato attivo sarà la parte che vorrà dimostrare la falsità del documento prodotto in giudizio, essendo tra l'altro indifferente la sua posizione, di attore o convenuto, di producente o di parte contro cui il documento è stato proposto, nel

---

l'accertamento della falsità ha eguali caratteristiche, sia nel processo penale di falso, sia in quello civile. Poiché nel processo penale si è certamente di fronte ad un mero accertamento, l'autore non ritiene possibile arrivare ad una conclusione diversa per il processo civile. Lo stesso autore sottolinea anche che la querela di falso può essere prodotta anche contro una scrittura privata non riconosciuta, cioè contro un documento che non ha il valore di prova legale: in questo caso il giudizio non può che avere un'efficacia di mero accertamento e costitutiva, in quanto non può essere diretto a togliere al documento l'efficacia di prova legale che non possiede.

[72] ATTARDI, *L'interesse ad agire*, Padova 1955. Tale autore è partito dal presupposto secondo cui la scrittura privata riconosciuta abbia la particolare efficacia di vincolare il giudice a quanto da essa risulta. Da ciò sarebbe possibile dedurre la natura costitutiva della querela di falso, in quanto diretta a privare la scrittura privata di tale efficacia

[73] DENTI, cit., pagg. 664 ss.

[74] MANDRIOLI, cit., pagg. 210 ss.

[75] DE STEFANO, cit., pagg. 696 ss.

giudizio principale. L'interesse a verificare ed accertare la veridicità di un documento potrebbe sorgere anche in capo al soggetto che ha prodotto il documento, giustificando così la legittimazione ad agire. Nel caso di querela principale, invece, la legittimazione attiva sembrerebbe spettare, soprattutto se si consideri la querela come un giudizio di accertamento, al titolare di un diritto sul documento. Non molte difficoltà ci sono nell'individuazione del soggetto legittimato passivamente, che va individuato non solo in colui che è parte del rapporto sostanziale dimostrato dal documento ma anche in colui che si trovi in una situazione, anche non ancora perfetta, per la quale il documento possa essere rilevante.

Non va dimenticato, infine, che anche per tale tipo di processo sarà necessario la presenza, così come stabilito dal codice di procedura civile, dell'interesse ad agire: cioè, per dirla con il Carnelutti, in tanto il processo si può azionare e il giudice può essere chiamato ad una decisione, in quanto ve ne sia bisogno.

Per quel che riguarda, invece, la compatibilità tra querela di falso e firma digitale, la dottrina, che si è occupata della questione[76], è d'accordo, anche se con sfumature diverse, nel dare una risposta affermativa, nel ritenere, cioè, che la querela di falso, viste le sensibili differenze rispetto al disconoscimento, possa avere ad oggetto la firma digitale.

Nell'analizzare la esperibilità della querela di falso verso un documento informatico sottoscritto con firma digitale è necessario distinguere due ipotesi: la prima è l'ipotesi base, cioè il caso in cui la firma digitale non sia autenticata, il secondo caso è, ovviamente, quello in cui la firma digitale sia stata autenticata. A prima vista si può affermare che la seconda ipotesi comporterà, a carico dell'attore, un onere probatorio molto maggiore rispetto al caso base.

L'esperibilità della querela di falso anche contro i documenti informatici muniti di firma digitale viene giustificata prendendo come presupposto la cosiddetta « teoria analitica della dichiarazione »: si è cioè affermato[77] che al fine della legittima formazione del documento dichiarativo, sia necessario distinguere le fasi (coessenziali) dell'« espressione » e dell'« emissione » del documento stesso. La paternità del testo, sulla base di questa tesi, non potrebbe prescindere dalla consapevole destinazione del documento ad altri; la prova dell'aver scritto non implica cioè la prova dell'avere dichiarato[78]. Si afferma, quindi, che per giungere alla piena prova della paternità del documento sarà necessario verificare anche l'emissione della scrittura, cioè la riferibilità all'au-

[76] Vedi, tra gli altri, FINOCCHIARO, cit., pagg. 983 ss.; DE SANTIS, cit., pagg. 392 ss.; GENTILI, cit., pagg. 174 ss.; ORLANDI M., cit., pagg. 874 ss.; REGGIANI, cit., pag. 1594; GRAZIOSI, cit., pagg. 516 ss.; ZAGAMI, cit., pagg. 179 ss.

[77] ORLANDI M., cit., pagg. 874-75.

[78] ORLANDI M., cit., pagg. 874-75.

tore della circolazione del documento. In altre parole, e con specifico riferimento al documento informatico munito di firma digitale, va ricordato che l'esigenza della querela di falso si pone perché la verifica tecnica non è in grado di individuare con certezza il reale autore del documento, ma sancisce, come visto, semplicemente un nesso oggettivo tra titolare delle chiavi certificate e firma digitale apposta al documento informatico, attraverso la presunzione (assoluta) di riferibilità, precedentemente esposta[79]. Essendo le chiavi, come gia detto, differentemente dalla sottoscrizione autografa, uno strumento tecnico e non un *quid* intimamente connesso con il sottoscrittore, possono astrattamente essere utilizzate da chiunque. Ecco che si giustifica l'esigenza di un accertamento ulteriore circa il reale autore della firma digitale. Per ottenere questa certezza è necessario proporre una querela di falso, tramite la quale non si dimostrerà la « falsità » della firma, bensì, diversamente, l'uso abusivo che altri abbiano fatto di questa.

Altra motivazione a sostegno dell'ammissibilità della querela di falso potrebbe essere individuata nel fatto che questa, ritenuto inammissibile il disconoscimento, rimarrebbe l'unico strumento processuale a disposizione del titolare della firma digitale per dimostrarne l'apocrifia.

Va, però, precisato, a titolo di premessa, che intanto si pone il problema della compatibilità della querela di falso con la firma digitale, in quanto il legislatore ha equiparato il documento informatico sottoscritto con firma digitale alla scrittura privata munita di sottoscrizione. Tale equiparazione costringe l'interprete ad individuare gli strumenti di difesa contro l'uso abusivo dello strumento elettronico di firma, necessari per garantire la sicurezza e la stessa diffusione su larga scala del nuovo mezzo di sottoscrizione, in un campo molto limitato di ipotesi, cioè all'interno delle soluzioni previste per la sottoscrizione autografa.

In altre parole si rende necessario ricordare che il problema nasce sostanzialmente da una mancanza del legislatore: questi dopo aver equiparato la firma digitale alla sottoscrizione autografa e, di conseguenza, il documento informatico con essa sottoscritto alla scrittura privata, non ha completato il lavoro, o, meglio, sembra non aver compreso sino in fondo la portata del nuovo tipo di documento e le sue enormi differenze rispetto a quello cartaceo. Il lavoro del legislatore sembra essersi fermato a metà: egli ha disciplinato soltanto l'aspetto sostanziale del documento informatico, tralasciando il momento patologico; tale incombenza, in ultima istanza, è stata assegnata agli interpreti, ai quali però non è stata

[79] Come gia detto *ante* nel testo, il documento informatico sottoscritto con firma digitale viene attribuito al titolare delle chiavi certificate con una sorta di evidenza pubblica.

data piena libertà di movimento nell'attività di ricerca all'interno dell'intero ordinamento di un mezzo di tutela non solo efficace ma anche tale da permetterne l'uso con la firma digitale senza dover essere stravolto nella sua essenza.

Tra questi mezzi di tutela, escluso il disconoscimento in quanto, come visto[80], ontologicamente incompatibile con la firma digitale, la principale, o meglio l'unica possibilità rimasta, è la querela di falso. Ai nostri fini non dovrebbe essere sufficiente considerarne e giustificarne l'utilizzazione esclusivamente in virtù di una necessità pratica di tutela, ma la sua applicabilità dovrebbe essere giustificata anche e soprattutto da un punto di vista teorico. In altre parole, va verificato se il mezzo processuale di cui trattasi viene considerato applicabile alla firma digitale in quanto unico e solo strumento, ultimo baluardo che l'ordinamento mette a disposizione dei titolari delle chiavi oggetto di abuso, ovvero perché si ritiene realmente possibile una sua utilizzazione senza che questo mezzo sia snaturato.

Obiettivo di questo scritto è proprio quello di dimostrare l'applicabilità della querela di falso alla firma digitale non solo perché questo strumento si configura come elemento necessario di difesa che l'ordinamento ha il dovere di approntare a favore di un soggetto che lamenti un'apocrifia, ma anche perché ci sono delle ragioni di tipo teorico con le quali motivare e sostenere tale conclusione.

Con questo non ho in animo di sancire la assoluta utilizzabilità della querela di falso ovvero, per meglio dire, della querela definibile « *pura* »[81] in riferimento alla firma digitale, o, meglio, al suo abuso; semplicemente ritengo necessario non solo affrontare i problemi con la dovuta obiettività e precisione, ma anche precisare che l'interpretazione proposta in questo testo non ha carattere di assolutezza, ma è un tentativo di affrontare la questione in termini problematici, certamente non privo di argomentazioni, ma comunque aperto al confronto. Vorrei nuovamente ricordare che, nell'interpretazione da me proposta, va tenuto ben presente che la scelta della querela di falso è stata fortemente indirizzata da una mancanza del legislatore, da un lato e dalla sua scelta di equiparare *sic et simpliciter* la firma digitale alla sottoscrizione autografa senza prevedere soluzioni per il momento patologico.

Oggetto della querela, almeno all'interno di un giudizio civile instaurato tra i due (presunti) sottoscrittori del contratto del quale si chiede l'adempimento, consisterà nel determinare, non tanto il reale autore della firma digitale, quanto che il titolare di questa

[80] Vedi *ante* nel testo.

[81] Intendendosi per pura la querela di falso così come disegnata originariamente dal legislatore nel cod. civ. e così come applicabile alla scrittura privata cartacea.

non la abbia utilizzata per sottoscrivere quel documento, cioè che quest'ultimo non è il reale autore della firma. I mezzi di prova a favore dell'attore (nel procedimento di querela di falso) sono liberi e consistono in quelli ordinari del nostro giudizio civile. Non è però possibile nascondere che in concreto sarà molto difficile riuscire a provare, in guisa da convincere il giudice, di non essere stato il reale utilizzatore della firma digitale; è infatti assolutamente complesso, specialmente nel caso in cui il contratto sia stato stipulato tramite la rete di internet, riuscire a dare la prova della quale il giudice avrebbe bisogno per dichiarare l'apocrifia della firma.

Nemmeno si pone il problema della preclusione rispetto a quanto è gia stato oggetto del giudizio di verificazione: seguendo l'interpretazione proposta in questo testo, che tende ad escludere il disconoscimento in caso di documento sottoscritto con firma digitale, tale problema assolutamente non si pone, in quanto la querela di falso è la prima ed unica sede dove dibattere della falsità del documento informatico; seguendo l'altra interpretazione, favorevole al disconoscimento ed alla successiva procedura di verificazione, il problema viene superato proponendo la classica[82] obiezione, secondo cui la querela di falso ha comunque un oggetto più ampio rispetto alla procedura di verificazione, per cui non è possibile parlare di sovrapposizione o di preclusione.

Per quel che riguarda la seconda ipotesi di querela di falso, cioè quella proposta contro un documento sottoscritto con firma digitale autenticata, è necessario fare una precisazione ulteriore rispetto a quanto detto fino a questo momento. L'autenticazione della firma permette, come gia detto, di stabilire con certezza il reale sottoscrittore, in quanto l'articolo 24 T.U. ha disposto che il notaio o il pubblico ufficiale autorizzato possono autenticare solo le firme digitali apposte in loro presenza e dopo aver accertato l'identità dei sottoscrittori. Questa considerazione non deve però ingannare: la più forte valenza probatoria della firma digitale autenticata non preclude la querela di falso, anche se, da un lato ne restringe l'oggetto, limitandolo all'ipotesi di falso ideologico da parte del notaio o del pubblico ufficiale autorizzato ed escludendo quindi la possibilità di provare l'abuso della chiave privata; dall'altro lato la rende più complessa di quanto già non lo fosse, sul piano probatorio: è evidente a tutti che dimostrare la falsità dell'attestazione del pubblico ufficiale sia un compito assolutamente proibitivo.

---

[82] MANDRIOLI, *Corso di diritto processuale civile*, Giappichelli editore, 1998, pagg. 210 ss..