Informatica e diritto, XXXIII annata, Vol. XVI, 2007, n. 1-2, pp. 193-221

Le prove informatiche e la produzione dei documenti probatori su supporto informatico

ALESSANDRA VILLECCO*

SOMMARIO: *1. Introduzione – 2. Le prove informatiche – 2.1. I documenti informatici – 2.2. La sottoscrizione dei documenti informatici – 3. L'acquisizione delle prove informatiche – 4. Il disconoscimento dei documenti informatici – 4.1. Il disconoscimento dei documenti informatici sottoscritti con firma elettronica – 4.2. Il disconoscimento dei documenti informatici sottoscritti con firma digitale – 5. Conclusioni*

1. INTRODUZIONE

Sono trascorsi dieci anni da quando con la legge 15 marzo 1997, n. 59 (c.d. legge Bassanini), il Governo veniva delegato ad emanare regolamenti per dare disciplina compiuta alla tecnica della documentazione informatica.

In questi anni, l'impiego della tecnologia informatica e di conseguenza l'uso dei documenti informatici, ha avuto ampia diffusione in diversi settori, sia in ambito pubblico sia privato. Nel settore pubblico, all'interno di quello che viene designato come fenomeno di *e-Government*, è proprio nell'àmbito dell'esperienza processuale che la tecnologia informatica è chiamata a svolgere un ruolo strategico: si parla della creazione di un processo telematico di un processo che si concreta in una sequenza di atti affidati alla tecnologia informatica, atti e documenti la cui efficacia e il cui valore giuridico diventa un prerequisito fondamentale.

Molteplici sono gli aspetti del processo informatizzato che vedono l'utilizzazione di atti digitali: si pensi, ad esempio, al verbale di causa, al fascicolo d'ufficio, ai provvedimenti del giudice ma anche alle notificazioni e alle comunicazioni.

Ma si pensi anche, ed è l'oggetto delle riflessioni svolte in queste pagine, all'utilizzazione degli strumenti informatici ai fini probatori: l'art. 14[1], in commento,

* Avvocato e Professore a contratto presso la Facoltà di Giurisprudenza dell'Università degli Studi di Verona. Docente in Master in diritto delle nuove tecnologie e informatica giuridica - Cirsfid - Bologna. Chair della Conferenza Internazionale *Computer aided-Law and Advanced Technologies* (CLAT).

[1] Art. 14 - *Produzione degli atti e dei documenti probatori su supporto informatico. - 1.* Gli atti e i documenti probatori offerti in comunicazione dalle parti dopo la costituzione in giudizio possono

disciplina in modo specifico, come risulta dalla stessa rubrica della disposizione normativa, la produzione in giudizio degli "atti e dei documenti probatori su supporto informatico", strumenti che devono essere qui studiati sia per quanto riguarda la loro tipologia, sia per i metodi di acquisizione, sia per la loro efficienza probatoria ai fini della formazione del convincimento del giudice.

2. Le prove informatiche

Ancora prima che il legislatore nazionale provvedesse, nel 1997[2], a dettare una disciplina sull'efficacia delle prove informatiche, il fenomeno della documentazione digitale era già largamente diffuso, in quanto diversi servizi e utenti, pubblici e privati, utilizzavano documenti prodotti da elaboratori elettronici[3].

Sin dal primo apparire della nuova tecnologia dottrina e giurisprudenza si erano subito occupate dei documenti informatici specie sotto il profilo

essere prodotti, oltre che per via telematica, anche mediante deposito in cancelleria del supporto informatico che li contiene. Il supporto informatico deve essere compatibile con i tipi e i modelli stabiliti al riguardo dal decreto di cui all'art. 3, co. 3, e deve contenere anche il relativo indice, la cui integrità è attestata dal difensore con la firma digitale. - *2*. Il responsabile della cancelleria procede a duplicare nel fascicolo informatico gli atti, i documenti probatori e l'indice indicati nel co. 1. - *3*. Il supporto informatico è restituito alla parte dopo la duplicazione di cui al co. 2.

[2] D.p.r. 20 novembre 1997, n. 513 Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'art. 15, co. 2, della legge 15 marzo 1997, n. 59 (Pubblicato nella G.U. 13 marzo 1998, serie generale, n. 60).

[3] I documenti creati dalla tecnologia informatica possono essere indifferentemente definiti informatici, elettronici o digitali, in quanto tali termini vanno intesi come sinonimi. Infatti, il documento informatico non è altro che il prodotto di un'elaborazione mediante computer redatto e conservato sotto forma di bit, non direttamente percepibile dall'uomo se non attraverso gli organi di output del computer, come il monitor o, in senso ancora più lato, nella sua produzione cartacea. Nel linguaggio del Codice dell'amministrazione digitale CAD il termine digitale assume uno specifico significato quand'è riferito al meccanismo di sottoscrizione, in quanto con il termine di firma digitale viene descritta una firma elettronica qualificata creata mediante il sistema di crittografia basato su una coppia di chiavi asimmetriche. Per documento elettronico deve intendersi non solo un testo, ma anche un'immagine o più immagini, un suono o più suoni o addirittura tutti questi insieme, come nell'ipotesi dell'opera multimediale. L'art. 1, lett. p) del d.lgs. 82/2005 definisce il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (la formulazione è identica a quella dei precedenti testi normativi). Tale rappresentazione avviene con la registrazione dei bit nelle memorie ausiliarie attraverso un procedimento di magnetizzazione o smagnetizzazione del supporto, oppure attraverso un procedimento di formazione o meno

della loro valenza probatoria[4]. Da una parte, furono considerate prove atipiche, quali mezzi probatori non espressamente contemplati da alcuna disposizione normativa ma comunque ammissibili, la cui efficacia poteva essere ricondotta a meri argomenti di prova; si ammetteva altresì che il giudice ben potesse conferire al documento informatico il valore di prova liberamente apprezzabile sufficiente comunque a fondare il proprio convincimento, purché di ciò desse adeguata motivazione. Tale orientamento fu poi superato per individuare la disciplina dell'efficacia dei documenti informatici in norme preesistenti da applicare per analogia, esattamente com'era stato fatto per il rilievo probatorio di telefax e telex utilizzando le norme in tema di efficacia probatoria delle copie fotografiche di scritture (art. 2719 c.c.).

Così, per quanto riguarda i documenti informatici, privi dell'ancora sconosciuta tecnica della firma digitale[5], si ritenne d'applicare per analogia la norma di cui all'art. 2712 c.c., con ciò stesso equiparando il documento informatico quanto al valore probatorio e quanto alle modalità di acquisizione come una riproduzione meccanica.

Solo con il citato d.p.r.. 513/1997, poi sostituito dal d.p.r. 445/2000 e, infine, con l'emanazione del Codice dell'amministrazione digitale (CAD) è stata emanata la disciplina sostanziale dell'efficacia dei documenti elettronici, divenuti così strumenti probatori tipici, non solo come mezzo probante, ma anche per il predeterminato criterio in base al quale il giudice deve valutarli[6].

di buchi nella superficie magnetica della memoria ausiliaria con un raggio laser. Questi segnali di varia natura magnetica, elettronica ed ottica costituiscono una forma di scrittura. Diversamente, il legislatore penale con l'art. 491-*bis*, co. 2, c.p. ha considerato contenere dati o informazioni con efficacia probatoria, sia i programmi informatici, sia il supporto informatico che contiene la prova informatica. Nella definizione di documento informatico l'elemento tecnico diviene essenziale per l'aspetto giuridico. La manifestazione di volontà di un individuo viene espressa non dal segno grafico della scrittura, bensì attraverso un procedimento che elabora dati trasferendoli su una memoria elettronica e solo l'intermediazione del computer ne rende possibile la percezione da parte dell'uomo. In argomento si veda M.G. LOSANO, *Scritto con la luce: il disco compatto e la nuova editoria elettronica*, Milano, Unicopli, 1988.

[4] G. VERDE, *Per la chiarezza delle idee in tema di documentazione informatica*, in "Rivista di diritto processuale", 1990, p. 715; L. MONTESANO, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, in "Rivista di diritto processuale", 1987, p. 5 ss.

[5] La firma digitale è stata disciplinata a partire dal d.p.r. 513/1997.

[6] In argomento si veda lo studio di G. VERDE, *Prove nuove*, in "Rivista di diritto processuale", 2007, p. 35.

Nel nostro ordinamento sussiste una caratteristica, la "duplicità disciplinare della *law of evidence*"[7], derivante dalla sua distribuzione fra codice sostanziale e codice di rito, ma si tratta di una disciplina che nell'ultimo mezzo secolo ha subito forti cambiamenti[8], ora particolarmente evidenti per effetto delle leggi che regolano gli strumenti probatori affidati alla tecnologia informatica.

È ben vero, peraltro, che la disciplina sulla documentazione elettronica ha seguito un percorso tutt'altro che lineare, come dimostrano i continui cambiamenti che non è opportuno ripercorrere in questa sede, se non per precisare che questa frastagliata, disomogenea e spesso poco chiara normativa ha ostacolato la diffusione e la utilizzazione dei documenti informatici ed ha causato, conviene notarlo, sfiducia e diffidenza negli operatori che hanno ostacolato, in particolare, il fruttuoso avvio del processo telematico.

A tal riguardo non ha dato certo un positivo contributo la prolifica tecnica delle definizioni che il legislatore ha sentito il bisogno di elaborare nel disciplinare gli istituti aperti alla tecnologia informatica: definizioni spesso incongrue e talora contraddittorie se non anche inutili.

Così, per fare un esempio, non si comprende l'esigenza di ripetere nel regolamento sul processo telematico la definizione di documento informatico già contenuta nei testi legislativi che espressamente lo disciplinano. Come è noto, il d.p.r. n. 123 del 2001 definisce documento informatico ogni "rappresentazione informatica del contenuto di atti, fatti o dati giuridicamente rilevanti ai sensi del d.p.r., 10 novembre 1997, n. 513" (art. 1 lett. a). Questa prima definizione del documento informatico, si affidava ad una formula incongrua, là dove essa si riferiva alla rappresentazione del "contenuto" dei fatti, è stata corretta dall'art. 1 lett. p) del CAD che ora definisce correttamente il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Le lettere successive del medesimo art. 1 definiscono, rispettivamente, il duplicato del documento informatico (lett. b) come "la riproduzione del documento informatico effettuata su un qualsiasi tipo di supporto elet-

[7] A. Dondi, V. Ansanelli, *Diritto delle prove e discrasie nella recente riforma italiana del processo civile*, in "Rivista trimestrale di diritto e procedura civile", 2007, p. 621.

[8] In argomento si veda L.P. Comoglio, *Riforme processuali e poteri del giudice,* Torino, Giappichelli, 1996, 332 p.; V. Denti, *Sistemi e riforme. Studi sulla giustizia civile,* Bologna, Il Mulino, 1999.

tronico facilmente trasportabile" e il documento probatorio (lett. c) come "l'atto avente efficacia probatoria ai sensi del codice civile e del codice di procedura civile". A questo proposito l'espressione "documento probatorio" e la definizione che ne viene data è pleonastica se non anche erronea, poiché è come scrivere d'una "prova probatoria": invero, ogni documento è per definizione mezzo di prova e, in particolare, mezzo di prova rappresentativa e ciò in quanto capace di dare la rappresentazione di dichiarazioni di scienza o di volontà[9] o di fatti o di cose[10].

Il documento può aver ricevuto *ex lege* una particolare efficacia, perché è stato formato da un soggetto abilitato a dare pubblica fede alla sua efficacia rappresentativa. Questo accade per i documenti che riproducono dichiarazioni attribuibili alla parte dichiarante: documenti quindi "dichiarativi" quali l'atto pubblico o la scrittura privata autenticata, ma anche la stessa scrittura privata, quando essa non viene contestata in giudizio. Ma il documento può essere non solo "dichiarativo", ma anche "rappresentativo" di fatti o di cose, nel caso in cui riproduca immagini, filmati o suoni, come avviene per le riproduzioni meccaniche disciplinate dall'art. 2712 c.c.

2.1. I documenti informatici

In un primo tempo, il legislatore ha ricondotto il documento informatico, ancora privo di qualunque tipo di firma elettronica[11], nell'àmbito delle riproduzioni meccaniche e della loro efficacia probatoria[12].

Il CAD non si occupa più di disciplinare direttamente l'efficacia del mero documento informatico, in quanto la norma contenuta nell'art. 21, e per l'appunto intitolata "Valore probatorio del documento informatico

[9] G.F. Ricci, *Diritto processuale civile, Il processo di cognizione e le impugnazioni*, II, Torino, Giappichelli, 2006, p. 89. In particolare sulla classificazione delle prove V. Denti, *Prova documentale*, in "Enciclopedia del diritto", XVIII, 1988.

[10] G.F. Ricci, *Diritto processuale civile, Il processo di cognizione e le impugnazioni*, *cit.*, p. 106.

[11] L. Montesano, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 1 ss. Anche per la giurisprudenza questa norma viene ritenuta riferita a tutte quelle rappresentazioni di fatti o cose frutto dello sviluppo tecnologico. In giurisprudenza; Cass., 16 febbraio 2004, n. 2912; Cass., 6 settembre 2001, n. 11445, in "Giurisprudenza italiana", 2002, p. 465 con nota di A.M. Socci, *La prova con i documenti informatici nella dinamica del processo.*

[12] Espressamente era scritto "ai sensi dell'art. 2712 c.c.", nel d.p.r. 513/1997 e nel successivo d.p.r. 445/2000.

sottoscritto", prende soltanto in considerazione i documenti muniti di firma sia digitale o elettronica qualificata sia elettronica semplice. Infatti, nel CAD non vi è più alcun rinvio all'art. 2712 sul valore probatorio del mero documento informatico: è questa stessa norma del codice civile che regola il valore probatorio del documento in questione, avendo l'art. 23 del CAD modificato l'art. 2712 c.c., che ora riconduce alle riproduzioni meccaniche anche le "riproduzioni informatiche".

Questa scelta non è priva di significato rispetto alla precedente regolamentazione, per cui ogni documento informatico, ancorché dichiarativo, veniva posto sullo stesso piano della riproduzione meccanica quanto all'efficacia. Sembrava così che si fosse attribuito valore a un documento scritto ma non sottoscritto, stravolgendo il sistema della prova documentale fondato sul valore attribuito alla sottoscrizione, un valore che si incentra sull'assunzione di paternità della dichiarazione documentata dalla scrittura sottoscritta, al punto che parte della dottrina aveva parlato d'una nuova categoria di prove[13].

Invero, nessun problema particolare pone il documento informatico come strumento tecnico in grado di rappresentare o fatti o cose e quindi come riproduzione meccanica nel senso reso esplicito dal testo dell'art. 2712, c.c. Più delicato e problematico ricondurre nell'àmbito di applicazione della medesima norma quei documenti informatici che sono veicolo di una dichiarazione di volontà, come nell'ipotesi d'un messaggio di posta elettronica: soluzione questa che veniva giustificata dall'interpretazione evolutiva dell'art. 2712 c.c., a cui venivano ricondotte le registrazioni magnetofoniche intese quali documenti riproduttivi di dichiarazioni non sottoscritte[14].

Ora invece, il nuovo testo dell'art. 2712, là dove riconduce alla disciplina delle riproduzioni meccaniche le riproduzioni informatiche, sembra

[13] G. VERDE, *Prove nuove*, *cit.*, 35 ss.; A. VILLECCO BETTELLI, *L'efficacia delle prove informatiche*, Milano, Giuffrè, 2004, p. 120 e p. 158 ss.

[14] "Si è più o meno ragionato: come la legge riconosce il valore probatorio della riproduzione della voce, espressamente contemplando le registrazioni "fonografiche" (e, per estensione, quelle magnetofoniche), così può dare rilievo alla conversione in documento scritto degli impulsi elettronici di cui si compone il documento elettronico." G. VERDE, *Prove nuove*, *cit.*, p. 41.

stabilire per implicito che il documento informatico privo di sottoscrizione può acquisire sul piano probatorio l'efficacia di piena prova solamente se rappresenta fatti o cose, salvo il disconoscimento da parte di colui contro il quale è prodotto. Se così fosse, ne deriverebbe che un semplice messaggio di posta elettronica non avrebbe valore di documento rappresentativo di una dichiarazione, ossia di documento rappresentativo alla stessa stregua delle prove scritte. Neppure la sede giudiziale e il contraddittorio tra le parti sarebbe idonea a conferire a tale documento valore probatorio per assenza di contestazione, in quanto tale regola è applicabile solo alle prove documentali tradizionali e, in particolare, alla scrittura privata, documento contenente una dichiarazione sottoscritta, oppure alla riproduzione meccanica, documento contenente la rappresentazione di fatti o cose.

In definitiva, bisogna concludere che ogni qual volta l'oggetto della prova è una dichiarazione espressione d'una manifestazione di volontà ed è contenuto in un documento che si forma attraverso il pensiero della mente umana[15], occorre, ai fini della sua efficacia probatoria, un segno tangibile d'assunzione di paternità da parte dell'autore. Collegamento questo che è stato ravvisato in tutti quei casi nei quali l'autore della dichiarazione abbia abbinato al documento informatico che la contiene una tecnologia forte in grado da rendere il documento medesimo inalterabile e sicuro, una scelta tecnica che implicherebbe l'assunzione di paternità della dichiarazione ivi documentata, salvo poi lasciare in ombra la risposta da dare all'interrogativo se questo dato tecnico possa garantire anche la sicura provenienza del documento.

Poco ausilio offre, sul punto, il legislatore, che nell'art. 20, co. 1-*bis*, CAD, ricollega i requisiti della sicurezza e della inalterabilità all'idoneità del documento informatico a soddisfare requisiti di forma e, in particolare, della forma scritta, e non anche al suo valore probatorio creando una divaricazione tra forma ed efficacia probatoria del documento informatico che le norme contenute negli articoli successivi, che espressamente disciplinano il valore probatorio del documento informatico sottoscritto con firma elettronica, non valgono a risolvere.

[15] A tal proposito si è parlato di prove indirette G.F. RICCI, *Diritto processuale civile, Il processo di cognizione e le impugnazioni*, *cit.*, p. 89.

A parere di chi scrive, l'utilizzazione di una tecnologia forte per la creazione del documento informatico dichiarativo soddisfa non soltanto i requisiti di forma, a cui fa riferimento il citato co. 1-*bis*, ma consente anche di fondare su di essa una presunzione di paternità tale da attribuire anche al documento informatico, privo di apparente sottoscrizione, il valore di documento sottoscritto elettronicamente anche sul piano probatorio, purché sia formato con una tecnologia che ne garantisca l'immodificabilità, l'inalterabilità e la provenienza, una prova documentale liberamente valutabile in giudizio, con le conseguenze che ne derivano e che sono esaminate nei paragrafi seguenti.

2.2. La sottoscrizione dei documenti informatici

L'esigenza di dare sicura soluzione al problema della paternità dei documenti informatici dichiarativi è stata affidata dal nostro ordinamento alla tecnologia della firma digitale: si tratta di una soluzione che successivamente è stata, come diremo, almeno in parte superata con la ricezione, attuata dal d.lgs. 10/2002, della direttiva comunitaria 1999/93/CE.

Prima della disciplina comunitaria sulle firme elettroniche, nel nostro ordinamento l'unica tipologia di firma abbinabile ad un documento informatico con il valore di sottoscrizione autografa era la firma digitale, la cui formazione tecnica era precisamente stabilita nelle modalità della crittografia asimmetrica.

La firma digitale[16] diversamente dalla firma elettronica tecnologicamente neutra, è stata affidata ad una tecnologia in cui sono addirittura coinvolti soggetti terzi, i certificatori (artt. 24-32), con un ruolo di responsabilità circa la determinazione del titolare della firma digitale: essi sono "parti fidate" che debbono possedere gli stessi requisiti di onorabilità richiesti agli ammi-

[16] Questa considerazione è resa in modo ancor più esplicito nel tutorial al *Digital Signature Guidelines – American Bar Association* (1996) ove chiaramente è scritto: "From an information security viewpoint, these simple electronic signature are distinct from the digital signatures described in this tutorial and in the technical literature, although digital signature is sometimes used to mean any form of computer-based signature. These Guidelines use digital signature only as it is used in information security terminology, as meaning the result of applying the technical processes described in this tutorial". Si veda inoltre lo Utah Digital Signature Act (1995-1996).

nistratori dalla legge bancaria[17]. Il CAD richiede, per dare alla firma digitale il massimo grado di efficacia, che la stessa sia basata su un certificato qualificato, che solo un certificatore qualificato, in possesso di determinati requisiti prefissati dalla legge e dai regolamenti, è in grado di rilasciare.

Tecnicamente la firma digitale è il risultato di una combinazione di algoritmi che utilizza il sistema della crittografia a chiavi asimmetriche, una pubblica ed una privata a cui il regolamento approvato dalla Presidenza del Consiglio dei Ministri del 13 febbraio 1999 (oggi abrogato e quasi integralmente assorbito dall'attuale regolamento tecnico il d.p.c.m. 13 gennaio 2004 in attesa delle nuove regole tecniche) ha abbinato la funzione matematica basata sull'*hash*.

Infatti, nel regolamento si usano termini come "impronta" e "funzione di *hash*" che, abbinati alle locuzioni verbali "dispositivo di firma" ed "evidenza informatica", dimostrano che la sottoscrizione con firma digitale deriva dalla crittografia asimmetrica e dalla funzione matematica di *hash*.

L'algoritmo della chiave privata viene dunque applicato alla stringa, cioè al sunto del documento ottenuto come risultato della funzione di *hash*. In tal modo il documento risulta firmato. Se si vuole ottenere anche la sua segretezza e quindi renderlo criptato, si potrà applicare la chiave pubblica di colui che si vuole rendere l'unico soggetto in grado di leggere quel documento.

Tutta questa operazione è ovviamente funzionale anche alla procedura di verifica della firma digitale, per dimostrare la coincidenza perfetta delle due impronte nel documento firmato digitalmente in modo valido[18].

Per la creazione della firma digitale, fino ad oggi, nel nostro ordinamento è stata data la preferenza al dispositivo *smartcard*[19], la c.d. scheda

[17] Infatti, negli Stati Uniti tali soggetti vengono definiti *Trusted Third Party*. Negli atti della *Digital Signature Guidelines dell'American Bar Association (1996)* e del *Signature Act dello Utah (1995-1996)* la *Trusted Third Party*, sembra svolgere un ruolo molto simile a quello del pubblico ufficiale che certifica l'apposizione della firma digitale in sua presenza, garantendo il legame tra firma digitale e suo titolare.

[18] Deliberazione CNIPA, 17 febbraio 2005, n. 4, *cit*.

[19] In altri contesti viene utilizzato un dispositivo che sfrutta l'ingresso mediante porta USB, come se si trattasse di un disco di memoria rimovibile, ad esempio una *pen drive*, contente all'interno il dispositivo di firma. Anzi, in futuro sarà sicuramente questa la strada prescelta, in quanto il dispositivo USB incorpora al suo interno i certificati digitali, le chiavi pubbliche e private,

intelligente, dotata di microchip contente i dati per la generazione della firma digitale e molto simile alla tessera del bancomat o della carta di credito. Questa tessera viene poi inserita in un apposito lettore e, previa immissione di un codice segreto (*pin* o *password*), rilascia le certificazioni elettroniche relative al suo utilizzatore.

Il recepimento della direttiva comunitaria 1999/93/CE con il d.lgs. 10/2002 ha determinato nel nostro ordinamento l'introduzione di altre tipologie di sottoscrizione dei documenti informatici e quindi di firme elettroniche ispirate al massimo grado di neutralità tecnologica[20].

Il legislatore comunitario ha voluto ampliare la tipologia degli strumenti di firma elettronica per far spazio a forme più semplici e ciò anche a prescindere da tecnologie forti tali da garantire l'immodificabilità e l'integrità di quanto creato col *medium* elettronico, salva la diversa rilevanza da attribuire a queste tecniche "leggere" sul terreno della graduazione del loro valore probatorio[21].

La firma elettronica può essere affidata ad un qualsiasi dato elettronico, ad esempio un semplice codice di identificazione (*pin*) oppure una parola chiave (*password*) logicamente connessa al suo titolare, ma anche stabilito con un accordo fra le parti che vogliano utilizzare la firma elettronica come metodo di sottoscrizione per i loro rapporti, insomma con una convenzione di firma che rientra nella previsione delle norme sulle forme convenzionali di cui all'art. 1352 c.c.[22].

2.2.1. Il documento con firma digitale

Il documento informatico munito di firma digitale si ottiene mediante l'apposizione della chiave privata del titolare-sottoscrittore al documento in base alle modalità tecniche descritte in precedenza. Le stesse

il *software* di creazione della firma, un *browser*; un sistema operativo indipendente da quello ospitante. Grazie a questo sistema l'utente non è obbligato ad installare *drivers* complessi, ma permette un uso facile e idoneo ad ogni *computer* supportato da porte USB.

[20] Anche l'UNCITRAL *Model Law on Electronic Signatures* - 2001, si è ispirato ad una tecnologia non forte e necessariamente predeterminata in relazione alle firme elettroniche semplici.

[21] In argomento si veda CONSIGLIO DI STATO, *Atti normativi*, in "Giurisprudenza italiana", 2005, n. 11995, con nota di A. LISI, G. LAZARI.

[22] A. VILLECCO BETTELLI, *L'efficacia delle prove informatiche*, *cit*., p. 122.

modalità tecniche consentono pure il procedimento inverso di verifica dell'autenticità della sottoscrizione.

Per le caratteristiche tecniche della firma digitale in precedenza esposte, il termine sottoscrizione, per quanto utilizzato dal legislatore, sembra difficilmente accettabile. Infatti, questa dovrebbe essere apposta alla fine del documento cui si riferisce, modalità possibile solo col documento cartaceo. Pertanto, è più corretto parlare di firma piuttosto che di sottoscrizione, anche se il legislatore utilizzando quest'ultimo termine ha voluto sottolineare la funzione precipua della firma elettronica, identica a quella della sottoscrizione: identificare con facilità l'autore dell'atto.

Il documento con firma digitale o con firma elettronica qualificata ai sensi dell'art. 21, co. 2, acquista l'efficacia probatoria di cui all'art. 2702 c.c.[23]. Il richiamo all'art. 2702 c.c. potrebbe destare qualche perplessità per i documenti informatici firmati con "firma digitale o con un altro tipo di firma elettronica qualificata", ma subito la norma inserisce una presunzione relativa, facilmente superabile con l'offerta della prova contraria, precisando che: "l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria". Il decreto legislativo del 2005 (CAD), richiamando espressamente la norma di cui all'art. 2702 c.c., così come aveva fatto il primo regolamento, il d.p.r. 513/97, sembra riaprire le questioni interpretative che avevano diviso la dottrina: in particolare, ci si chiedeva se tale richiamo dovesse essere inteso come un generico richiamo alla scrittura privata e quindi all'astratta tipologia della prova documentale, oppure anche alla disciplina, dettata dall'art. 2702, per quanto riguarda l'efficacia probatoria e le condizioni affinché tale efficacia possa dispiegarsi.

Nel primo caso, la forza probatoria privilegiata sarebbe immediatamente riconosciuta al documento elettronicamente sottoscritto mentre, nel secondo, sarebbero necessarie quelle attività integrative (riconoscimento o mancato disconoscimento giudiziale, ovvero l'autenticazione

[23] Il regolamento contenuto nel d.p.c.m. 13 gennaio 2004 sulle regole tecniche sul documento informatico all'art. 3, co. 3, dispone che "Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma, non produce gli effetti di cui all'art. 10, co. 3, del testo unico, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati."

della sottoscrizione da parte del pubblico ufficiale) per dare al documento informatico efficacia di prova legale sulla provenienza delle dichiarazioni sottoscritte.

A prima vista, anche per quanto espresso in passato da dottrina e giurisprudenza[24], sembrerebbe preferibile la prima soluzione. Conviene peraltro notare che la presunzione *iuris tantum,* di cui nella seconda parte del co. 2 dell'art. 21, quale presunzione del controllo sul dispositivo di firma, rafforza l'idea che il legislatore abbia voluto ricondurre la valenza probatoria del documento informatico munito di firma digitale o di altro tipo di firma elettronica qualificata solo parzialmente ai precetti dell'art. 2702 c.c.

Infatti, la possibilità data alla parte di disconoscere il documento contro di lei prodotto, dimostrando di non essere stata nelle condizioni di aver utilizzato il dispositivo di firma per la creazione della firma digitale, apre chiaramente la possibilità di una contestazione sulla provenienza del documento con firma digitale o altra firma elettronica qualificata, un disconoscimento che ha il suo parallelo in quanto dispongono gli artt. 214 e ss. c.p.c. Una contestazione che ben potrebbe seguire le vie del giudizio di falso sull'uso illegittimo della firma digitale se a questa venisse data l'efficacia privilegiata, che gli attribuiva l'originario 10, co. 3, del d.p.r. 445/2000: "il documento informatico, quando e' sottoscritto con firma digita [...] fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto"[25].

Anche il CAD, ossia il più volte citato d.lgs. n. 82 del 2005, precisa che, qualora la firma digitale o un altro tipo di firma elettronica qualificata sia basata su un certificato elettronico revocato, scaduto o sospeso, il docu-

[24] In argomento si veda A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, in "Rivista trimestrale di diritto e procedura civile", 1998, p. 515 "ammettere la possibilità di disconoscimento della firma digitale significherebbe, per certi aspetti, addossare alla parte che produce il documento informatico un onere probatorio quasi diabolico. Poiché, non potendosi ovviamente far ricorso alle scritture di comparazione, i mezzi istruttori a disposizione di colui che instaura il procedimento di verificazione della scrittura privata per provare l'autenticità della firma digitale disconosciuta sarebbero veramente ridotti al minimo".

[25] Su questi ragionamenti si veda M. Orlandi, *L'imputazione dei testi informatici*, in "Rivista del notariato", 1998, p. 872; R. Zagami, *Firma digitale e sicurezza giuridica nel d.p.r. 10 novembre 1997, n. 513 e nel d.p.c.m. 8.2.1999*, Padova, Cedam, 2000; A. Villecco Bettelli, *L'efficacia delle prove informatiche*, *cit*., p. 129.

mento si considera non firmato. Ovviamente tramite gli elenchi pubblici, che il certificatore ha l'obbligo di tenere, tutto ciò che concerne la sorte del certificato relativo alla firma digitale deve essere debitamente reso noto attraverso forme di pubblicità costitutiva. Infatti, la revoca o la sospensione, comunque motivate, hanno effetto solo dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, possa dimostrare che tutte le parti interessate erano già a conoscenza di tale fatto.

2.2.2. Il documento con firma elettronica

Nell'evoluzione della disciplina normativa del documento informatico, il documento con firma elettronica è sempre stato inteso quale prova liberamente valutabile dal giudice ed idoneo a soddisfare il requisito della forma scritta, oltre a consentire l'adempimento degli obblighi di tenuta delle scritture contabili previsti dall'art. 2214 c.c. (art. 10, d.p.r. 445/2000)[26].

Anche l'attuale disciplina dettata dall'art. 21 CAD riconosce efficacia di prova liberamente valutabile al documento sottoscritto con firma elettronica semplice. Il giudicante nel suo giudizio valutativo da esprimere con congrua motivazione, dovrà tenere conto se il meccanismo di creazione della firma elettronica rispetta alcuni parametri di qualità e sicurezza, seppur minimi, tali da attribuire affidabilità della stessa. In questo contesto possono valere le considerazioni sul documento informatico con firma elettronica quale nuovo strumento di prova[27], nel

[26] Trib. Cuneo, 29 gennaio 2004, ha ritenuto che un messaggio di posta elettronica possa costituire la prova scritta ai sensi dell'art. 633 c.p.c. quale presupposto all'emissione di un decreto ingiuntivo, in quanto il messaggio di posta elettronica, che contiene una promessa unilaterale di debito, costituisce documento informatico firmato elettronicamente. Per il giudice piemontese ha costituito firma elettronica ai sensi dell'art. 10, co. 2, d.p.r. 445/2000 *username* e *password* che si digitano per accedere alla propria casella di posta elettronica per poter creare ed inviare un messaggio *e-mail*, eseguendo in questo modo "un'operazione di validazione" […] e tale documento soddisfa altresì il requisito legale della forma scritta, a norma del combinato disposto degli artt. 1, co. 1, lett. cc) e 10, co. 2 del d.p.r. 445/2000. Ancora Trib. Ancona, 9 aprile 2005, che considera come prova scritta *ex* art. 648 c.p.c., ai fini del diniego della provvisoria esecuzione del decreto ingiuntivo opposto, l'intercorsa "corrispondenza, trasmessa via *fax* ed *e-mail* a sostegno della domanda riconvenzionale spiegata dall'opponente per il riconoscimento della pretesa di credito vantata nei confronti dell'opposto".

[27] G. Verde, *Prove nuove*, *cit*., pp. 42-43; A. Villecco Bettelli, *L'efficacia delle prove informatiche*, *cit*., pp. 163-164.

senso che si tratta di un documento dichiarativo sottoscritto che non è stato equiparato alla scrittura privata quanto al valore probatorio ed ai meccanismi di verifica della sua autenticità, bensì ritenuto prova liberamente valutabile circa il suo stesso contenuto. Infatti, quello che la firma elettronica dovrebbe garantire con un certo grado di attendibilità è la provenienza del contenuto, non costituire invece una prova liberamente valutabile della dichiarazione stessa. Al contrario, la formula normativa sembra dare rilevanza allo stesso contenuto delle dichiarazioni documentate con lo strumento informatico, come se, attraverso l'accertamento della genuinità del documento contenente la dichiarazione, si ritenesse veritiera anche la dichiarazione; una valutazione questa che il giudice non può certo "ricavare dalla struttura dello strumento con cui essa viene conservata, ma da circostanze e valutazioni diverse"[28].

2.2.3 Il documento con firma digitale autenticata

L'apposizione della firma autografa ad un documento può avvenire dinanzi ad un pubblico ufficiale che ne dà attestazione con autentica fino a querela di falso che il sottoscrittore è stato identificato con atto avente valore di atto pubblico. Al pari della firma autografa, anche la firma digitale costituisce manifestazione di volontà di dichiarare la paternità dell'atto cui viene apposta e, sempre al pari della firma autografa, può essere autenticata, garantendo fino a querela di falso l'identità soggettiva di chi la appone.

Il codice dell'amministrazione digitale richiama espressamente l'art. 2703 c.c. sull'autenticazione della firma autografa da parte del pubblico ufficiale; esso deve preventivamente accertare l'identità personale del titolare, la validità del certificato elettronico ed il fatto che il documento sottoscritto corrisponde alla volontà della parte, senza essere in contrasto con l'ordinamento giuridico ai sensi dell'art. 28 legge notarile[29].

L'autenticazione avviene sempre da parte di un notaio o altro pubblico ufficiale a ciò autorizzato e, per ora, non è contemplata la possibilità di eseguire tale procedura a distanza attraverso soluzioni tecniche che possano ovviare alla compresenza fisica del sottoscrittore e del pubblico ufficiale.

[28] In questi termini, G. VERDE, *Prove nuove*, *cit.*, p. 43.

[29] M. DI FABIO, *Manuale di notariato,* Milano, Giuffrè, 1981.

3. L'acquisizione delle prove informatiche

Il Regolamento sull'uso degli strumenti telematici e informatici nel processo civile e amministrativo nel disciplinare all'art. 14 la produzione degli atti e dei documenti probatori su supporto informatico al co. 1 dispone che: "gli atti e i documenti probatori offerti in comunicazione dalle parti dopo la costituzione in giudizio possono essere prodotti oltre che per via telematica, anche mediante il deposito in cancelleria del supporto informatico che li contiene"

Sull'imprecisione lessicale circa le definizioni, come "documenti probatori", si è già fatto cenno in precedenza. In questo contesto occorre invece rilevare come la norma faccia riferimento non solo al materiale che viene offerto in prova, ma anche all'attività di comunicazione fra le parti degli atti processuali che in qualche modo rientrano nell'attività istruttoria, come ad esempio la richiesta di ammissione di una prova: invero "comunicare" e "produrre" sono verbi utilizzati dalla norma che si riferiscono, rispettivamente, agli atti processuali ed alle deduzioni probatorie.

In questa sede non ci si soffermerà sull'analisi degli atti processuali[30], in quanto tale argomento è già oggetto di disamina nel commento all'art. 4 del d.p.r. 123/2001 (vedi, in questo volume, il contributo di G. Briganti), ma solo in relazione all'attività istruttoria delle prove informatiche e delle attività processuali ad esse correlate.

Nell'ipotesi contemplata dall'art. 14, co. 1, del d.p.r. 123/2001 le modalità attraverso le quali è possibile depositare i documenti sono due. La prima prevede la trasmissione telematica; la seconda, il deposito presso la cancelleria del supporto in grado di contenere il documento informatico, una scelta che può anche dipendere essenzialmente dal formato dell'originale.

È anzi probabile che se il documento nasce in formato digitale, la sua produzione in giudizio avverrà quasi certamente con trasmissione *online*, e la trasmissione avrà ad oggetto, lo si noti, il documento originale in forma digitale e non una sua copia. Diversamente, quando il documento da produrre è cartaceo, per essere trasmesso in via telematica dovrà previamente essere scansionato e pertanto la trasmissione avrà ad oggetto la copia del documento originale.

[30] A. Villecco, *Le notificazioni e le comunicazioni telematiche nel processo civile. Posta elettronica e telefax*, Bologna, Gedit, 2007, p. 37 ss.

Occorre peraltro tenere presente che la trasmissione telematica significa trasmissione a distanza di documenti in modo automatico mediante impulsi elettronici: in questo caso vi rientrerebbe anche il telefax come mezzo di trasmissione a distanza. Si può osservare che il regolamento del 2001 sul processo telematico fa espresso riferimento non soltanto a strumenti legati alla tecnologia informatica, di conseguenza al *computer* e a Internet, ma anche – come si legge nella stessa intitolazione della legge – all'uso di strumenti telematici il che consente con certezza di utilizzare anche il telefax come mezzo idoneo di comunicazione, come del resto prevede in più luoghi lo stesso codice di rito civile.

A identiche conclusioni si approda anche quando avviene il deposito in cancelleria del supporto informatico. Anche in questo caso il deposito non ha ad oggetto il documento originale cartaceo, ma il supporto elettronico sul quale è stato previamente salvato previa scansione. Per utilizzare il linguaggio degli estensori delle regole tecniche questa procedura è definita di conservazione sostitutiva e ciò per la ragione che il documento originale o la copia che s'intende produrre nasce non digitale, bensì in modo analogico. Il legislatore ha qui avuto cura di precisare che "il supporto informatico deve essere compatibile con i tipi e i modelli stabiliti al riguardo dal decreto di cui all'art. 3, co. 3" e che "deve contenere anche il relativo indice, la cui integrità è attestata dal difensore con la firma digitale".

I "tipi di modello" di supporto informatico che contengono la prova, cui fa riferimento la norma, sono quelli con parametri tecnici che garantiscono una conservazione duratura e inalterabile del dato digitale in base alle regole tecniche affidate, a norma dell'art. 3, co. 3, a provvedimenti ministeriali, avallati dal CNIPA, in conformità con l'art. 2, co. 15, della l. 24 dicembre 1993, n. 537 e del Codice dell'amministrazione digitale in materia di documenti della pubblica amministrazione[31].

Per la sicura conservazione dei documenti informatici è prevista la procedura di validazione temporale che consiste nella generazione di una marca temporale applicata ad un'evidenza informatica e generata da un apposito sistema elettronico sicuro, che ai sensi dell'art. 44 CAD deve

[31] In particolare, la conservazione dei documenti informatici, così come la loro formazione e trasmissione, sono stabiliti con regolamento ministeriale ed ora l'ultimo in ordine di tempo è il d.p.c.m. 13 gennaio 2004, che ha integralmente sostituito quello dell'8 febbraio 1999.

essere in grado di: a) mantenere la data e l'ora; b) generare la struttura di dati che deve contenere una serie di informazioni specifiche e deve essere generata da una coppia di chiavi asimmetriche; c) sottoscrivere digitalmente la struttura di dati di cui alla lettera b). La conservazione può anche avvenire con la memorizzazione su supporti ottici mediante l'impiego della tecnologia *laser*, come ad esempio i dischi ottici, i magneto-ottici, oppure i DVD, idonei a garantire la conformità dei documenti all'originale, in base alle regole espresse nella deliberazione CNIPA n. 11 del 19 novembre 2004, che completa la disciplina tecnica sulla conservazione dei documenti informatici[32].

La cautela manifestata dal legislatore, evidenzia con chiarezza l'intenzione di preferire la trasmissione online del materiale probatorio, proprio perché il processo telematico mira a privilegiare questa tecnica, perfettamente in sintonia con la sua struttura e architettura, e con le esigenze di garanzia da esse presupposte già soddisfatte dalla considerazione che l'integrità e la provenienza dei documenti trasmessi sono attuate dai meccanismi della firma digitale o della posta elettronica certificata.

Ne deriva che la produzione di documenti con deposito in cancelleria si pone come eccezione rispetto alla regola della loro trasmissione telematica. Infatti, per produrre in cancelleria fisicamente il supporto informatico, non solo occorre utilizzare dei correttivi tecnici per un'adeguata e legale conservazione del documento, ma occorrono anche ulteriori formalità, come l'indice con l'elenco dei mezzi di prova depositati con supporto digitale, e sottoscritto con la firma digitale del difensore e ciò non solo per certificare i documenti depositati, ma anche per attestarne l'integrità.

Il rientro nelle procedure del processo telematico, è attuato dai successivi adempimenti del cancelliere. La duplicazione da parte del responsabile della cancelleria nel fascicolo informatico degli atti, dei documenti probatori e dell'indice, dimostra che non rimangono presso la cancelleria atti o documenti che non possono confluire nel fascicolo digitale o in quello cartaceo speculare, poiché dopo l'operazione di riversamento sostitutivo il supporto informatico è restituito alla parte dopo la duplicazione.

[32] I.P. CIMINO, *L'archiviazione ottica dei documenti: presupposti normativi, lineamenti e aspetti operativi*, in "Diritto dell'Internet", 2005, p. 511.

In questo caso il responsabile della cancelleria dovrà apporre una marca di riferimento digitale dell'avvenuta memorizzazione delle prove informatiche sul fascicolo informatico, nonché la propria firma digitale e sarebbe auspicabile che di detto deposito vi fosse una certificazione da destinare alla parte che ha effettuato il deposito e ciò anche mediante l'inoltro contestuale di una *e-mail* certificata alla casella di posta del difensore.

Un discorso specifico merita la lettura dei dati informatici trasmessi come mezzi di prova. È opportuno distinguere tra il documento informatico ed il documento informatico sottoscritto digitalmente. In base all'attuale tecnologia sulla verifica dell'apposizione della firma digitale, poiché la chiave pubblica del sottoscrittore è contenuta nel certificato digitale che accompagna il documento informatico firmato, non si rendono necessarie particolari attività istruttorie per "leggere" il documento informatico, come pure è stato detto al punto che si era parlato di prova costituenda e della necessità di fissare un'udienza *ad hoc* per la loro assunzione[33]. Si consideri, infatti, che la visione da parte del giudice di un documento informatico riproduttivo di un'immagine, di un video, oppure di un audio, non richiede certo particolari attività istruttorie, sempreché, s'intende, il magistrato abbia *computers* dotati di *software* idonei a visualizzare con sicurezza il dato informatico.

Nell'auspicabile prospettiva d'un processo telematico pienamente funzionante, mi sembra da abbandonare l'idea che le prove digitali debbano essere assunte con l'attivazione di un esperimento giudiziale ai sensi dell'art. 261 c.p.c., senza che questo possa comportare violazione del contraddittorio nell'acquisizione della prova.

In assenza di un processo informatizzato secondo i parametri tecnici e di sicurezza dettati dal d.p.r. 123/2001 e dai successivi regolamenti tecnici, la produzione di un documento informatico in sede giudiziale che avvenga con il deposito del supporto in cancelleria rischia di creare ostacoli più che vantaggi: infatti, nell'impossibilità pratica di eseguire le modalità di duplicazione ai sensi dell'art. 14, si renderebbe necessario estrarre una copia cartacea ai fini di una più semplice consultazione ad opera del giudice[34]; opera-

[33] A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, *cit.*, p. 481 ss.

[34] Con la realizzazione del processo telematico questo aspetto potrebbe venire risolto dalla cancelleria per la coesistenza del fascicolo cartaceo accanto a quello informatico.

zione questa che potrebbe anche esigere l'applicazione dell'art. 261 c.p.c. e indurre il giudice ad avvalersi dell'opera di un esperto. Qualora, invece, il documento informatico per le sue caratteristiche ontologiche non sia trasferibile su supporto cartaceo, come nel caso di un compact disk che contenga una registrazione di un suono, di un filmato o di un brano musicale, in sede giudiziale occorrerà far ricorso alla procedura descritta nell'art. 259 c.p.c. sull'ispezione di riproduzioni meccaniche in modo da assicurare altresì il pieno contraddittorio fra le parti.

4. Il disconoscimento dei documenti informatici

L'efficacia del documento informatico non sottoscritto è ora regolata dall'art. 2712 c.c., per cui se non ne viene disconosciuta la capacità rappresentativa, fa piena prova dei fatti e delle cose che riproduce, al pari di ciò che accade per le riproduzioni fotografiche[35]. Il disconoscimento del documento informatico sarebbe dunque regolato dal codice di rito con una disciplina identica a quella del disconoscimento della virtù rappresentativa delle riproduzioni meccaniche.

Su tale meccanismo di reazione all'efficacia della prova documentale informatica, potrebbe influire notevolmente l'eventualità che si possa prospettare una graduazione della sua efficacia probatoria, un'efficacia da determinare caso per caso, considerando le caratteristiche tecniche del documento informatico e la possibilità che venga modificato o alterato sia quanto alla provenienza sia quanto al suo contenuto.

In concreto, il giudice potrebbe trovarsi nella condizione di valutare discrezionalmente il grado di attendibilità della prova informatica anche considerando la qualità della parte che produce la prova. Infatti, la possibilità di manipolare un documento informatico può dipendere anche dalla posizione in cui un soggetto, si trova per proprie specifiche competenze: si pensi all'amministratore di sistema che ha libero accesso a quasi tutte le informazioni, per esempio ai log di posta elettronica, e quindi si trova nella possibilità materiale di modificare i dati[36].

[35] Trib. Trapani, 31 maggio 2002, in "Giurisprudenza di merito", 2003, p. 1444.

[36] A. Villecco Bettelli, *L'efficacia delle prove informatiche*, *cit*., pp. 120-121, in particolare sul ragionamento in merito alle prove atipiche.

Come si è detto, la parte contro cui è prodotto il documento può contestare la conformità ai fatti e alle cose che vi sono rappresentate. Ma è dubbia la sorte del documento informatico disconosciuto: si potrebbe pensare che perda ogni efficacia, in analogia con quanto accade alla scrittura privata, ma anche che sia pur sempre un mezzo di prova sia pure affidato alla libera valutazione del giudice.

La dottrina maggioritaria[37] propende chiaramente per la prima interpretazione salvo ammettere che il giudice, in caso di contestazione, possa disporre una consulenza tecnica per accertare la genuinità della prova. La Cassazione ha costantemente sostenuto che il disconoscimento delle riproduzioni meccaniche, previsto dall'art. 2712 c.c., sia diverso dal disconoscimento della scrittura privata di cui all'art. 215 c.p.c.: invero, la riproduzione meccanica disconosciuta non impedisce al giudice di accertarne la conformità all'originale anche attraverso altri mezzi di prova, incluse le presunzioni, diversamente da quanto accade nell'ipotesi di scrittura disconosciuta che, se non viene instaurato, il giudizio di verificazione non può essere utilizzata[38].

In tal senso si sono orientati i giudici di legittimità in riferimento all'interpretazione della norma di cui all'art. 5, co. 2 d.p.r. 513/97[39]. Sulle conclusioni cui è pervenuta la Cassazione in questa circostanza si sono levate le critiche da parte della dottrina[40] che esclude recisamente che la rappresentazione meccanica di cui all'art. 2712 c.c. possa acquistare il valore di una prova liberamente valutabile una volta che sia stata disconosciuta

[37] L. MONTESANO, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 7; G.F. RICCI, *Valore probatorio del documento informatico ed errori duri a morire*, in "Rivista trimestrale di diritto e procedura civile", 2002, p. 1423.

[38] Cass., sez. lav., 6 settembre 2001, in "Jurisdata".

[39] Cass., 11445/2001, cit. In particolare nella motivazione si legge: "[…] le norme del codice civile sul disconoscimento della conformità all'originale di copie fotostatiche non autenticate di una scrittura si applicano solo quando questa sia fatta valere come negozio per derivarne direttamente e immediatamente obblighi, e non anche quando il documento sia esibito al solo fine di dimostrare un fatto storico da valutare nell'apprezzamento di una più complessa fattispecie, restando in tal caso il giudice libero di formarsi il proprio convincimento utilizzando qualsiasi circostanza atta a rendere verosimile un determinato assunto, come qualsiasi altro indizio, purché essa appaia grave, precisa e concordante". Nello stesso senso anche Cass., 25.1.1999, n. 659.

[40] G.F. RICCI, *Valore probatorio del documento informatico ed errori duri a morire*, *cit.*, p. 1423.

e quindi ammettere che i fatti oggetto della rappresentazione possano essere provati anche con altre prove, comprese le presunzioni.

Giova infine ricordare che per un prevalente orientamento interpretativo, il disconoscimento previsto dall'art. 2712 c.c., non soggiace agli stessi limiti temporali voluti dall'art. 215 c.pc., potendo essere esercitato in qualunque momento[41]: ma sul punto si registrano anche opinioni discordi[42].

Per ciò che concerne il procedimento di verificazione di cui all'art. 216 c.p.c., la dottrina non è concorde sulla sua utilizzazione per superare il disconoscimento della riproduzione meccanica[43]. Significativa appare a tal proposito l'opinione espressa da uno studioso particolarmente attento alla problematica in questione per cui "se la parte nei cui confronti la riproduzione viene fatta valere la disconosce, essa non acquista il valore di prova legale e la definizione della sua efficacia probatoria viene affidata al prudente apprezzamento del giudice"[44].

È dunque nel caso di contestazione di un documento informatico che possono essere attivati i procedimenti giudiziali per accertare la conformità della riproduzione informatica ai fatti o alle cose in essa rappresen-

[41] F. CARNELUTTI, *Prova fotografica e fonografia,* in "Rivista di diritto processuale", 1942, I, p. 233; E.T. LIEBMAN, *Manuale di diritto processuale civile (Principi)*, Milano, Giuffrè, p. 366; L. MONTESANO, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 5; L.P. COMOGLIO, *Le prove civili*, Torino, Utet, 2004, p. 290; E. GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, Giuffrè, 1984, p. 160; V. DENTI, *La verificazione delle prove documentali*, Torino, Utet, 1957, p. 79.

[42] F. DE SANTIS, *Il documento non scritto come prova civile,* Napoli, ESI, 1988, p. 142; F. LUCIFERO, *Riproduzioni meccaniche, copie ed esperimenti*, in "Enciclopedia del diritto", XL, Milano, 1989, p. 1084.

[43] Ritengono applicabile analogicamente l'art. 216 c.p.c. L. MONTESANO, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 8; F. DE SANTIS, *Il documento non scritto come prova civile, cit.*, p. 51; di diverso avviso F. LUCIFERO, *Riproduzioni meccaniche, copie, ed esperimenti*, *cit.*, p. 1084; V. DENTI, *La verificazione delle prove documentali*, *cit.*, p. 79. in giurisprudenza Cass. 15.5.1987, n. 4479, in "Massimario giur. it.", 1987.

[44] S. PATTI, *Della tutela dei diritti,* voce Della prova documentale, a cura di Galgano, in *Commentario del codice civile* diretto da Scialoja e Branca, Bologna-Roma, 1996, p. 128. Del resto è stato anche ipotizzato che in questo caso si sarebbe in presenza di un principio di prova per iscritto tale da poter derogare al limite della prova testimoniale e per presunzioni ai sensi dell'art. 2729, co. 2, c.c. in materia di contratti R. BORRUSO, *Computer e diritto*, Milano, Giuffrè, 1988, p. 235; E. GIANNATONIO, *Manuale di diritto dell'informatica*, in "Diritto scienza e tecnologia", diretto da Giannantonio e Rescigno, Padova, Cedam, 1997, p. 396.

tate, e questo per attuare, anche sotto questo profilo, l'eventuale parallelismo con il sistema di norme che disciplinano i meccanismi per ristabilire l'efficacia della scrittura privata disconosciuta. Così si è giustamente pensato che a fronte di un disconoscimento della riproduzione meccanica è possibile utilizzare tutti gli strumenti istruttori che consentano al giudice di valutare la contestata conformità della riproduzione: già si è detto dell'esperibilità d'una consulenza tecnica o di un esperimento giudiziale *ex* art. 261 c.p.c.[45] nel pieno rispetto del principio del contraddittorio.

Nel caso poi vi fosse un rifiuto ingiustificato della parte di cooperare alla verifica tecnica, potrebbero aversi conseguenze significative sul piano probatorio e ciò in quanto la parte porrebbe in essere un comportamento valutabile come argomento di prova ai fini della decisione e ciò ai sensi dell'art. 116, co. 2, c.p.c.[46].

Aperta rimane comunque la questione sull'efficacia da attribuire al documento informatico dopo il riconoscimento o l'esito favorevole del procedimento giudiziale di accertamento della veridicità della prova. Invero, quale potrà essere il valore da attribuire alla riproduzione meccanica così "integrata" dall'esito positivo dell'esperimento giudiziale; un valore di piena prova come avviene nel caso della scrittura privata oppure valore di prova liberamente valutabile dal giudice[47]?

A tal proposito si possono ricordare le conclusioni di quella dottrina[48] che non condivide la giurisprudenza orientata a negare che la riproduzione meccanica disconosciuta possa acquistare il valore di prova liberamente valutabile una volta che sia stata disconosciuta. Infatti, è la legge che ha voluto evitare tale conseguenza, stante la simmetria istituita con l'art. 2702 c.c. che si riferisce alla scrittura privata legalmente riconosciuta e fa perdere ogni efficacia alla scrittura medesima qualora venga disconosciuta: tale effetto deve valere anche nell'ipotesi dell'art. 2712 c.c., altri-

[45] G.F. Ricci, *Aspetti processuali della documentazione informatica,* in "Rivista trimestrale di diritto e procedura civile", 1994, p. 868; L. Montesano, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 5.

[46] F. De Santis, *Il documento non scritto come prova civile*, cit., p. 60.

[47] F. Carnelutti, *La prova civile,* rist. Milano, 1992, p. 233; L. Montesano, *Sul documento informatico come rappresentazione nella prova civile e nella forma negoziale*, *cit.*, p. 1.

[48] G.F. Ricci, *Valore probatorio del documento informatico ed errori duri a morire*, *cit.*, p. 1423.

menti in entrambe i casi la prova diventerebbe piena fino a querela di falso. Non a caso la scrittura privata disconosciuta può ancora produrre un'efficacia probatoria piena se viene sottoposta con successo al giudizio di verificazione, mentre nulla in tal senso è previsto per quanto riguarda le riproduzioni meccaniche.

4.1. Il disconoscimento dei documenti informatici sottoscritti con firma elettronica

Il documento informatico sottoscritto con la sola firma elettronica, ai sensi dell'art. 21 CAD è liberamente valutato dal giudice "tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità". La firma elettronica assurge *ex lege* a metodo di firma e nel contempo soddisfa il requisito legale della forma scritta.

Se si accoglie l'orientamento che dà a questo requisito il valore che contraddistingue determinate tipologie di documenti come la scrittura privata o l'atto pubblico, saremmo di fronte ad una nuova tipologia documentale che pur essendo firmata con un metodo assolutamente non sicuro di identificazione del sottoscrittore, ha comunque un'efficacia probatoria liberamente valutabile dal giudice, e presumibilmente, circa la provenienza del documento[49].

Se così fosse, allora, si dovrebbe pensare ad una possibilità di disconoscimento ad opera della parte contro cui è prodotto il documento informatico con firma elettronica, parte che non avrebbe quindi l'onere di disconoscere, ma non anche quello di dare prova contraria. Contro il disconoscimento, che toglierebbe ogni efficacia alla prova in questione, sarebbe eventualmente esperibile una sorta di giudizio di verificazione con i medesimi effetti previsti per la verificazione della scrittura privata, per cui il documento informatico così sottoscritto e favorevolmente verificato, acquisirebbe l'efficacia di piena prova. Ma questo epilogo sembra contrastare l'intenzione del legislatore che non ha voluto sicuramente attribuire al documento informatico con firma elettronica il medesimo valore della scrittura privata, avendo il legislatore semplicemente disposto che tale produzione informatica "soddisfa il requisito legale della

[49] Si rinvia a quanto in precedenza sostenuto nel capitolo sesto del volume A. VILLECCO BETTELLI, *L'efficacia delle prove informatiche*, *cit.*

forma scritta"[50], e che, sotto il profilo probatorio, è prova liberamente valutabile dal giudice.

Infatti, la firma elettronica non ha i medesimi effetti, quanto all'imputazione della paternità, propri del documento con firma digitale o con firma elettronica qualificata, entrambe in grado di garantire le medesime finalità della sottoscrizione autografa. Anzi, il meccanismo per la generazione della firma digitale ha un *quid pluris* rispetto alla sottoscrizione autografa, poiché produce l'effetto ulteriore della non riutilizzabilità della sottoscrizione e ciò nel senso che, per ragioni di carattere meramente tecnico, l'apposizione della firma digitale al documento non è da questo scindibile, in quanto essa varia al variare del contenuto del testo, a prescindere che venga applicata con la medesima chiave privata[51], tenendo comunque presente che la firma digitale può essere apposta, ovvero contenuta nello stesso file del documento, oppure associata. Questa peculiare caratteristica la differenzia dalla mera sottoscrizione elettronica che può avvenire con l'allegazione di dati in forma elettronica, oppure con l'associazione logica ad altri dati e quindi con un qualsiasi dato elettronico riconducibile al *computer*.

La sottoscrizione autografa proprio per il suo carattere personale di natura somatica assolve la funzione probatoria di provenienza del documento, pertanto gli strumenti volti ad accertare o a negare tale efficacia della sottoscrizione hanno ad oggetto l'accertamento dell'autenticità della sottoscrizione ed in alcuni casi anche della scrittura[52]. Con il disconoscimento la parte nei cui confronti è prodotto il documento nega formalmente la propria scrittura o la propria sottoscrizione; di conseguenza la parte che intende valersi del documento disconosciuto ha l'onere di instaurare il procedimento di verificazione, producendo scritture di comparazione al fine dimostrare la coincidenza del segno grafico nella firma del sottoscrittore del documento sottoposto a verifica e a questo scopo il giudice può altresì ordinare alla parte di scrivere sotto dettatura alla pre-

[50] F. DE SANTIS, *Tipologia e diffusione del documento informatico*, in "Corriere giuridico", p. 389.

[51] G. FINOCCHIARO, *Firma digitale e firme elettroniche,* Bologna, 2002, p. 68, nota 8; F. RIZZO, *Valore giuridico ed efficacia probatoria del documento informatico*, in "Il diritto dell'informazione e dell'informatica", 2000, p. 217.

[52] B. CARPINO, *Scrittura privata,* in "Enciclopedia del diritto", XLI, Milano, Giuffrè, 1989; L.P. COMOGLIO, *Le prove civili*, *cit.*, p. 194.

senza di un tecnico[53]. La simbologia grafica in questo caso gioca un ruolo determinante in relazione all'efficacia probatoria della scrittura privata.

Ciò non può certo verificarsi nell'ipotesi della firma elettronica dove si dovrà dare la prova, da un lato, dell'accordo in base al quale le parti avevano attribuito alla firma elettronica il valore di sottoscrizione; dall'altro, che il titolare di quella firma elettronica l'abbia sicuramente apposta quale espressione della sua volontà di concludere quel contratto ai sensi di quegli accordi sulle convenzioni di firma *ex* art. 1352 c.c.; questa verifica potrà anche utilizzare indici presuntivi, al pari di quelli che accompagnano l'esame grafologico nel giudizio di verificazione.

4.2. Il disconoscimento dei documenti informatici sottoscritti con firma digitale

L'attuale formulazione dell'art. 21, co. 2, CAD, per cui "l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria", è da intendersi come l'ammissione del disconoscimento nei confronti di un documento informatico con firma digitale, stante il richiamo all'art. 2702 c.c. circa l'efficacia probatoria di tale documento.

Nel senso che se non viene esercitato questo tipo di disconoscimento legato alla prova di un abusivo utilizzo della chiave privata per mancata disponibilità del dispositivo di firma, è pienamente provata la paternità dello stesso fino a querela di falso.

In concreto, si avrebbe una sorta di anticipazione del giudizio di querela di falso, più che di un tipico procedimento di verificazione della scrittura privata, nel senso che ciò che deve essere accertato è la provenienza del documento circa la tecnica di creazione, e non l'autenticità della firma digitale in sé[54]. Anche l'istruzione probatoria in questa incidentale fase di accertamento della veridicità della prova si atteggia in modo diverso. Innanzitutto, l'inversione dell'onere della prova in capo al soggetto contro cui è proposto il giudizio di verificazione, in virtù della presunzione *juris tantum* di titolarità della firma digitale al titolare del dispositivo di generazione della firma medesima, in secondo luogo, un'istruzione probatoria fondata su qualunque tipo di prova, perché non vi sono limiti di

[53] V. Denti, *La verificazione delle prove documentali*, *cit.*

[54] G. Verde, *Prove nuove*, *cit.*, p. 44.

ammissibilità neppure alla prova testimoniale per dimostrare la sottrazione o l'abusivo utilizzo del dispositivo per generare la firma digitale, qualora non si renda necessaria un'indagine tecnica.

Il ripudio della sottoscrizione digitale in sede giudiziale può avvenire solo nell'ambito di un giudizio di falso a causa della natura tecnica della firma digitale, diversamente dalla firma autografa che è un dato prettamente personale. Questa componente tecnica della sottoscrizione è stata definita come manifestazione della c.d. spersonalizzazione imputabile allo strumento informatico[55].

La procedura di validazione che attesta legalmente la provenienza del documento consiste in un procedimento di verificazione della provenienza, oltre che dell'integrità, del documento informatico[56]. L'algoritmo della chiave privata e, di conseguenza, la firma digitale devono riferirsi in maniera univoca ad un solo soggetto così come dimostra il certificato qualificato. La chiave pubblica invece serve a verificare il messaggio e dunque l'autenticità del documento.

A rigore, nulla vieterebbe, secondo la logica della presunzione di provenienza adottata dal *Digital Segnature Act* dello Utah (sec. 46.3.406) e dalle *Digital Segnature Guidelines* dell'ABA (par. 5.6), che il presunto firmatario, a seguito della produzione del documento firmato unitamente alla chiave pubblica, nonché ad un valido certificato per la verifica della firma, nel corso di questa procedura, potesse disconoscerla dimostrando che lui non è il sottoscrittore effettivo e quindi di vincere la presunzione di provenienza.

Secondo qualche autore, è proprio partendo da una presunzione di provenienza soggettiva della firma gravante sul soggetto che risulta titolare del certificato della chiave pubblica, che si identifica l'autore della firma e si evita di porre a carico di chi produce la scrittura (documento informatico) un onere probatorio eccessivamente gravoso, che risulta apertamente in contrasto ai principi, e tale da vanificare il meccanismo della firma digitale e dell'infrastruttura a chiave pubblica. Se così fosse, la mera "titolarità di un certificato di chiave pubblica con cui si verifica una firma digitale comporterebbe, dun-

55 G. Finocchiaro, *Firma digitale e firme elettroniche*, *cit.*, p. 116.

56 C.M. Bianca, *Il contratto,* in "Diritto civile", III, Milano, Giuffrè, 2000, p. 305.

que, di per sé una presunzione di responsabilità e riferibilità di tutte le firme con esso verificabili"[57].

Peraltro, se il giudizio di verificazione si risolvesse semplicemente nella verifica tecnica della firma e nell'individuazione del soggetto titolare del relativo certificato, non vi sarebbe alcun spazio per il presunto soggetto firmatario di dimostrare il contrario nell'ambito dello stessa fase processuale di verificazione. Infatti, come già precisato, la procedura di verifica della firma digitale e quindi della corrispondenza tra chiave privata e pubblica, non può che avvenire allo stato dell'attuale tecnica con la procedura informatica di validazione[58] che non necessita di procedimenti giudiziali in contraddittorio tra le parti[59]: oggetto della procedura di verifica è semplicemente la corrispondenza tra la chiave privata utilizzata per apporre la firma digitale avanzata e la chiave pubblica, di cui può essere titolare soltanto un soggetto determinato[60]. Tuttavia, l'univocità della firma digitale viene ad essere garantita soprattutto dalla tecnica adottata[61]: già la lunghezza prestabilita della chiave privata a partire da 1024 bit, rende praticamente impossibile che vi siano due chiavi private identiche[62].

Può però verificarsi nell'utilizzo della tecnica di *hash* nella firma digitale che una firma generata dalla chiave privata di un soggetto e dal documento cui è apposta possa coincidere con la firma generata da un altro

[57] R. ZAGAMI, *Firma digitale e sicurezza giuridica nel d.p.r. 10 novembre 1997, n. 513 e nel d.p.c.m. 8.2.1999*, *cit.*, p. 178.

[58] G. FINOCCHIARO, *Firma digitale e firme elettroniche*, *cit.*, p. 67.

[59] Gli strumenti informatici del giudice dovrebbero essere dotati di dispositivi per la verifica della firma (art. 1, lett. *mm*), che consistono in programmi informatici (*software*) oppure in apparati strumentali come *hardware* usati per la verifica della firma, al fine proprio di poter verificare l'apposizione di una firma elettronica qualificata ad un documento informatico.

[60] L'esclusiva assegnazione della chiave privata ad un determinato soggetto deve essere controllata dal certificatore, in capo al quale sussiste l'obbligo di rigettare la richiesta in caso di anomalie, così come hanno stabilito i vari regolamenti tecnici.

[61] Alcuni problemi sotto il profilo della procedura di certificazione potrebbero sorgere in relazione al quadro internazionale in assenza di accordi di certificazione.

[62] Anche la nuova disciplina è per l'univocità della firma elettronica qualificata, così come altre fonti di regolamentazione a livello internazionale come la *Draft Uniform Rules on Electronic Signature* (riportate in UNCITRAL, Working Group on Electronic Commerce, Thirty-second Session (Vienna, 19-30 January 1998), *Draft Uniform Rules on Electronic Signature* (A/CN.9 /WG.IV/WP.73, 12 December 1997, par. 23).

soggetto sul medesimo documento o su un altro documento[63]. È da domandarsi se di fronte ad una ipotesi come questa sia ammissibile un disconoscimento da far rientrare nell'ipotesi dell'art. 21, co. 2, seconda parte, oppure, poiché non si tratta di un mancato utilizzo del dispositivo di firma digitale da parte del suo titolare, si possa far venire meno l'efficacia piena solo con querela di falso.

Il giudice, in questo caso di contestazione, dovrebbe fissare un'udienza per sperimentare la provenienza della firma (non esistendo invero altro sistema). In tale sede, potrà provvedere personalmente alle operazioni di verifica con l'ausilio di un elaboratore elettronico, facendo redigere apposito processo verbale delle attività compiute: il giudice dovrà dare atto, in particolare, di aver constato il risultato positivo o negativo della procedura di controllo, allegando agli atti, eventualmente, il riscontro cartaceo rilasciato dall'elaboratore e controfirmato dal giudice medesimo[64].

La verifica della firma digitale di un documento informatico prodotto in giudizio non può, dunque, essere effettuata unicamente nell'ambito di un "sistema informatico e crittografico" mediante un apposito *software*

63 B. SCHNEIER, *Applied Cryptography. Protocols, Algorithms and Source Code in C.,* 2 ed., 1996, New York, Wiley, p. 38, ha scritto "One-Way Hash Function […] Speed increases drastically and, since the chances of two different documents having the same 160-bit hash are only two in 2160 , anyone can safely equate a signature of the hash with a signature of the document".

64 In base al nuovo regolamento il certificatore ha una serie di obblighi tra i quali vi è anche quello di non rendersi depositario dei dati per la creazione della firma del titolare, infatti questi devono essere nella esclusiva disponibilità del titolare (art. 28 lett. *e*), come si evince anche dall'art. 1 in riferimento ai codici o chiavi crittografiche private, ovvero i dati per la creazione di una firma. Ricostruendo i vari passaggi dell'indagine del giudice, il primo dovrebbe riguardare il certificato allegato alla firma digitale (art. 11, regolamento tecnico), da cui si può verificare la firma medesima applicando la chiave pubblica di sottoscrizione corrispondente a quella privata utilizzata per apporre la firma. Questa verifica, però, richiede un preliminare controllo sull'autenticità e validità del certificato: quest'ultimo infatti potrebbe essere falso, oppure aver perso la sua validità, a causa della sua scadenza, revoca o sospensione. Tali informazioni dovrebbero essere reperite dal giudice sia dal certificato stesso sia dal registro dei certificati, per verificare la pubblicazione di eventuali revoche o scadenze dei certificati rilasciati. Poiché il certificato è firmato con la chiave privata di certificazione del certificatore, la verifica si effettua applicando la corrispondente chiave pubblica (di certificazione). Tutta questa serie di operazioni deve essere facilitata dal certificatore stesso attraverso efficienti sistemi che consentano una rapida e facile consultazione dei dati raccolti dal certificatore stesso anche e soprattutto per via telematica.

fornito dal centro tecnico, ma anche mediante un controllo che può articolarsi in vario modo. Ai sensi dell'art. 261, co. 3, c.p.c. il giudice potrà eventualmente affidare l'esecuzione ad un perito[65] e soprattutto dallo stato della tecnica, in particolare in riferimento ai *software* utilizzati in sede di verifica delle firma digitali[66].

5. Conclusioni

Nel processo informatizzato l'istruzione probatoria basata su prove informatiche non subisce particolari modifiche rispetto alla disciplina dell'attuale codice di rito: invero, non si rendono necessari particolari procedimenti istruttori affinché il giudice possa consultare il materiale probatorio prodotto sia online, sia depositato materialmente in cancelleria su supporto informatico e poi fatto confluire nel fascicolo informatico. Infatti, le applicazioni informatiche di cui devono essere dotati i dispositivi tecnici a disposizione dei magistrati nel processo telematico consentono validamente l'intelligibilità dei documenti informatici siano questi sottoscritti o no. Diversamente, in caso di contestazione dovranno essere attivate procedure nel contraddittorio delle parti che consentano un'indagine tecnica appropriata circa la verifica di veridicità delle prove contestate o disconosciute, procedure che allo stato attuale non sono disciplinate dal regolamento del 2001, ma dal codice di procedura civile.

A tal riguardo non si può fare a meno di pensare che questi procedimenti dovranno probabilmente essere adattati per meglio garantire l'indagine tecnica sotto il profilo sia delle attività che devono essere espletate, sia per l'attività di documentazione di ciò che accade nel corso di dette indagini.

[65] A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, *cit.*, p. 511.

[66] L.P. Comoglio, *Le prove civili*, *cit.*, p. 183.