Dialoghi di Diritto dell'Economia

Ottobre 2014

ARTICOLI

La firma elettronica: problemi e prospettive

Enea Franza
Roberto Rossi

DB

La firma elettronica: problemi e prospettive

Enea Franza e Roberto Rossi

1. Premessa[01]

Come è noto l'atto giuridico consiste in un comportamento umano volontario rilevante per l'ordinamento giuridico. L'atto assume rilevanza nel momento in cui viene esternato, ossia reso visibile ad altri soggetti. Il mezzo con il quale viene portato a conoscenza di altri costituisce la *forma* dell'atto[02].

Quando è richiesta la forma scritta l'atto viene esternato per mezzo di un *documento*[03], che in passato veniva redatto su un supporto cartaceo ed oggi anche su supporto informatico.

Per gli atti giuridici, a differenza dei meri fatti, è rilevante "l'*imputazione*" ossia la riconducibilità dell'atto ad un soggetto, che può essere una persona fisica o una persona giuridica per conto della quale la persona fisica agisce in qualità di organo.

Il modo ordinario mediante il quale l'autore dell'atto se ne assume la paternità è la sottoscrizione che consiste nell'apposizione della firma in calce all'atto[04]. La sottoscrizione deve essere sempre apposta di pugno dall'autore come un segno personale[05] e deve essere tale da consentire l'individuazione con

01 Le opinioni degli autori sono espresse a titolo personale e non coinvolgono l'Autorità presso cui gli stessi lavorano.

02 Carnelutti – Sistema del diritto processuale civile, II, pag. 160, esprime efficacemente il concetto affermando che: "volontà è il pensiero in quanto si traduce in movimento, cioè la forza fisica; insomma lo spirito si incarna. Sotto questo profilo si chiarisce il significato della parola forma: forma vuol dire la parte esterna di un ente è quasi il vaso o lo stampo, entro il quale la essenza si contiene; questa essenza è la volontà".

03 Per documento si intende un oggetto materiale idoneo a rappresentare o far conoscere un fatto. In tal senso cfr. Mandrioli – Corso di diritto processuale civile, vol II, pag. 192 – Giappichelli editore.

04 Secondo Carnelutti – La prova civile, ristampa, 1992, pp.42-43, la creazione del documento non consiste nell'atto materiale della sua formazione, bensì nell'atto giuridico mediante il quale se ne assume la paternità. In tal senso cfr. anche Guidi – Teoria giuridica del documento, 1950, pag. 30.

05 In dottrina, cfr. Carpino – Scrittura privata, in Enc. dir., XLI, 1989, pag. 809, è stato sostenuto che esiste una differenza fra sottoscrizione e firma. La prima consisterebbe nell'indicazione del nome e del cognome, mentre la seconda potrebbe consistere anche in un'abbreviazione. Un altro autore, Carpino – Scrittura privata, in Enc. Dir., XLI, 1989, pag. 809, ha affermato che, mentre la firma rappresenterebbe una partecipazione senza alcuna connessione al testo a cui si riferisce, la sottoscrizione rappresenterebbe una manifestazione di volontà di aderire al contenuto dell'atto. Nella prassi i due termini sono considerati sinonimi.

Per quanto riguarda la firma illeggibile, le Sezioni Unite della Corte di Cassazione, 11-09-1979, n. 4746, ne ammettono la validità nei casi in cui il segno apposto sia tale da consentire l'identificazione del soggetto e la non riproducibilità della firma stessa.

ragionevole certezza della persona che l'ha vergata[06].

2. Avvento dell'informatica

Con l'avvento dell'informatica l'importanza del supporto cartaceo è venuta sempre più a ridursi e i documenti sono stati via via trasformati in *file*, creati e conservati su un *computer*, molto più maneggevoli del documento cartaceo. Rimaneva, però, un problema fondamentale: quello relativo alla sottoscrizione del documento.

Il documento informatico, infatti, doveva essere stampato e sottoscritto dall'autore. Pertanto la rivoluzione informatica non era ancora riuscita ad eliminare del tutto il supporto cartaceo con i relativi problemi di spedizione e conservazione. Paradossalmente per ogni documento informatico esisteva il doppione cartaceo.

Il problema è stato risolto mediante l'istituzione della firma elettronica che non obbliga più il redattore dell'atto a stamparlo per farlo sottoscrivere al soggetto a cui si riferisce.

Era, però, necessario compiere un passo ulteriore consistente nel conferire valore giuridico al documento informatico e dalla firma elettronica, equiparandola *in toto* alla tradizionale sottoscrizione posta in calce all'atto, conferendole la medesima capacità di attestare con certezza l'integrità, l'autenticità e la non ripudiabilità del documento[07].

3. Codice dell'amministrazione digitale

Nella fase antecedente all'entrata in vigore del D.lgs. 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale"(di seguito CAD)[08], la rilevanza giuridica del documento informatico era stata presa in

06 In tal senso cfr. Comoglio – Le prove civili, in Trattato di diritto privato, XXXI, ristampa, 1999, pag. 194.

07 Il percorso è stato alquanto tormentato. Nel 1997 il legislatore italiano, primo al mondo, aveva sancito con l'art. 15, c. 2 della legge 59/97 la validità e rilevanza del documento informatico "a tutti gli effetti di legge". Due articoli del regolamento applicativo, il DPR 513/97 (che disciplinava solo la firma digitale "sicura") sancivano in modo inequivocabile l'equivalenza del documento informatico al documento cartaceo. Dopo il recepimento della direttiva 1999/93/CE, operato con il D.Lgv. 10/02, e con il recentissimo DPR 137/03, questi due pilastri sono crollati.

08 "Commento al D.Lgs. 82/2005 dopo le modifiche apportate" Realizzato dal Digital & Law Department Studio Legale Lisi col patrocinio di ANORC e FORUM PA – Giugno 2014, Edizioni FORUM PA.

considerazione in modo sporadico e frammentario soltanto da alcune norme (ad esempio: art. 22, legge 7 agosto 1990 n. 241 sul procedimento amministrativo, l'art. 234 c.p.p. in tema di prova documentale, ecc.).

Successivamente la legge 15 marzo 1997, n. 59 (nota con il nome di Bassanini 1) ha stabilito il principio generale secondo cui gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge (art. 15, comma 2).

Il CAD, regolando in modo organico la materia, ha gettato le basi per la dematerializzazione dei documenti. Per dematerializzazione si intende il processo mediante il quale un documento viene creato e conservato utilizzando supporti di natura informatica[09]. L'obbiettivo del legislatore è stato quello di conferire validità giuridica all'attività amministrativa e contrattuale svolta con l'ausilio di strumenti informatici. Il documento "dematerializzato", conforme alla disciplina dettata dal CAD, ha lo stesso valore giuridico e probatorio di quello cartaceo.

Va, peraltro, precisato che, la disciplina in materia di strumenti informatici e firme elettroniche, pur essendo contenuta all'interno del CAD, quindi in una legge destinata prevalentemente alla pubblica amministrazione, trova applicazione anche nei rapporti fra privati.

La disciplina sulla dematerializzazione si riferisce sia ai documenti creati direttamente in formato elettronico che a quelli creati in formato cartaceo e successivamente trasformati in documenti informatici (c.d. *"conversione analogico-digitale)*.

Il documento elettronico, definito dal Codice come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", costituisce un elemento indispensabile per la dematerializzazione dell'attività amministrativa[10].

09 Vedi in particolare, "Le nuove frontiere del documento informatico e della firma elettronica: dalla firma digitale attraverso quella grafometrica fino alla "mobile signature", di avv. Andrea Lisi - Coordinatore Digital & Law Department, tratto da Sistemi&Impresa n.4 - aprile/maggio 2012.

10 L'art. 1, comma 1, lett. p) del CAD definisce il documento informatico come *"la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*. La successiva lettera p-*bis*) contiene la definizione del documento analogico, inteso come *"la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*.

Il CAD, entrato in vigore il 1° gennaio 2006, si prefigge lo scopo di assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando, con le modalità più appropriate, le tecnologie dell'informazione e della comunicazione (art. 2, comma 1).

Pochi mesi dopo l'entrata in vigore, il CAD è stato sottoposto ad una serie di correttivi apportati con il D.lgs. 4 aprile 2006, n. 159 che ha modificato diversi articoli.

Successivamente, il D.L. 185/2008, convertito in legge n. 2/2009 (c.d. *"Decreto anti crisi"*) ha apportato modifiche ai commi 4 e 5 dell'art. 23 conferendo alla copia con firma digitale lo stesso valore dell'originale senza l'obbligo di autentica da parte di un notaio o di altro pubblico ufficiale.

Altre modifiche sono state apportate con la legge 18 giugno 2009, ma le modifiche e le integrazioni più importanti sono state introdotte dal D.lgs. 30 dicembre 2010, n. 235 che ha modificato 53 articoli sui 92 originari introducendone altri 9.

Le ultime modifiche in ordine di temposono quelle apportata dal D.L. 18 ottobre 2012, n. 179, convertito con modificazioni con legge 17 dicembre 2012, n. 221, dal D.L. 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98 e dalla legge 27 dicembre 2013, n. 147.

3.1 Opinioni contrastanti

L'entrata in vigore del CAD non è stata unanimemente accompagnata da giudizi positivi da parte degli operatori e della dottrina[11]. Infatti, mentre alcuni autori hanno considerato il CAD un importante atto di riordino della materia, altri, invece, né hanno sminuito la portata innovativa sostenendo che in esso sono contenute molte enunciazioni di principio non accompagnate da disposizioni operative che né consentano la concreta attuazione.

Altri ancora hanno contestato il collocamento della disciplina sul documento informatico la cui sede naturale avrebbe dovuto essere il Testo Unico sulla documentazione amministrativa (D.P.R. n.

11 Cfr.Codice della P.A. digitale: cosa cambia per il cittadino ?, su www.webimpossibile.net; capire il codice dell'amministrazione digitale e cosa accadrà nelle P.A., idem; Codice della P.A. digitale: accessibilità ed usabilità dei siti istituzionali, idem; Il diritto all'utilizzo delle nuove tecnologie nel codice dell'amministrazione digitale, idem.

445/2000) dove l'atto in forma elettronica avrebbe potuto essere disciplinato insieme all'atto cartaceo, come alternativa a quest'ultimo.

Secondo altri[12], infine, il CAD sarebbe venuto meno al suo intento iniziale, che era quello di utilizzare l'informatica come strumento di semplificazione dell'attività amministrativa, sottovalutando i rischi del passaggio improvviso e non graduale dal supporto cartaceo a quello elettronico, creando in tal modo una discriminazione fra i cittadini abituati ad utilizzare strumenti informatici e quelli che, non essendo esperti, avrebbero avuto maggiori difficoltà a dialogare con la pubblica amministrazione in via telematica (c.d. *Digital Divide*).

3.2 Tipologie di firma elettronica

Il CAD prevede quattro tipologie di firma:

- la firma elettronica pura e semplice, che consiste nell'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1,lett. q);

- la firma elettronica avanzata intesa come insieme di dati, allegati oppure connessi tramite associazione logica a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1, lett. q-*bis*);

- la firma elettronica qualificata, che costituisce un particolare tipo di firma elettronica avanzata,è basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1, lett. r);

- la firma digitale che costituisce anch'essa un particolare tipo di firma elettronica avanzata,

12 Bissanti G. e Copello M. – Il *Digital Divide* nelle campagne italiane, Roma 2008; Bentivenga S. – Disuguaglianze digitali; le nuove forme di esclusione nella società di informazione, ed. Laterza 2009; Gui M. – Le competenze digitali. Le complesse capacità d'uso dei nuovi media e le disparità nel loro possesso, Napoli 2009; Anzera G. e Comunello F. – Mondi digitali. Riflessioni e analisi sul *Digital Divide*, Milano; Calderaro A. – *Digital Divide*, l'informazione nelle dinamiche tecno-economiche, su Rivista di cultura politica "InnoVazioni", 6, gennaio-febbraio 2006.

basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, lett. s).

Nelle applicazioni pratiche si sono inoltre diffuse alti due tipi di firme: la firma grafometrica, che consiste nell'apposizione di una sottoscrizione autografa su un particolare *tablet* e la firma apposta tramite *"one time password"* (password usata una sola volta).

La firma grafometrica, utilizzata in Spagna sin dal 2010, è anch'essa un particolare tipo di firma elettronica avanzata e consiste in una procedura informatica che permette di rilevare la firma autografa tramite un supporto tecnologico (*tablet* o *pad*). In altri termini, il soggetto appone la propria firma su una tavoletta grafica all'interno della quale sono predisposti appositi dispositivi che capaci di acquisirla rilevando l'immagine della firma, il ritmo, la velocità, la pressione, l'accelerazione e il movimento. La misurazione dei suddetti parametri permette di identificare, in modo abbastanza certo, l'identità del soggetto che firma. E' valida a tutti gli effetti di legge. Pertanto, anche se apposta su un *tablet* o *smartphone* ha lo stesso valore legale della tradizionale firma apposta sul foglio di carta.

L'OTP *(One Time Password)* è uno strumento delle dimensioni di un portachiavi che consente di generare una password usa e getta di alcune cifre valida per confermare determinate operazioni mediante la digitazione di un pulsante. Il dispositivo consente:

- la firma semplice;

- la firma elettronica. In questo caso le password da utilizzare per la firma vengono create successivamente alla digitazione delle cifre.

Per poterle considerare come firme elettroniche avanzate, con conseguente attribuzione del valore giuridico e dell'efficacia probatoria ex art. 21 CAD, è necessario che siano strutturate in modo tale da

garantire le condizioni richieste dalle regole tecniche previste dagli artt. 56 e 57[13], altrimenti saranno considerate firme elettroniche pure e semplici.

La differenza tra la firma elettronica pura e semplice e quella avanzata è, pertanto, nel "collegamento" dei dati. Nella firma elettronica pura e semplice i dati elettronici sono allegati o connessi ad "altri dati", che vengono poi utilizzati per l'identificazione informatica, mentre in quella avanzata i dati sono collegati ad un "documento informatico" e consentono l'identificazione del firmatario del documento.

La firma elettronica qualificata e quella digitale, invece, sono particolari tipologie di firma avanzata.

La prima si basa su un "certificato qualificato" (e non su un "documento informatico" come quella avanzata) rilasciato da un certificatore in possesso di specifici requisiti e iscritto in un elenco tenuto dall'AgID ed è realizzata mediante un dispositivo sicuro per la creazione della firma.

La seconda, invece, si basa su un "certificato qualificato" come la precedente e su un sistema di chiavi

13 Art. 56 *"Caratteristiche delle soluzioni di firma elettronica avanzata: 1. Le soluzioni di firma elettronica avanzata garantiscono:*
a) l'identificabilità del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
h) la connessione univoca della firma al documento sottoscritto.
2. La firma elettronica avanzata generata in violazione di quanto disposto da una o più disposizioni di cui alle lettere a), b), c), d), e), g), h) del comma 1, non soddisfa i requisiti previsti dagli articoli 20, comma 1-bis, e 21, comma 2, del Codice".
Art. 57 *"Moduli e formulari: 1. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica l'elenco della documentazione richiesta per singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.*
2. Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati; in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli e formulari. La mancata pubblicazione è altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili".

crittografiche.

In altri e più chiari termini, la firma elettronica pura e semplice si associa al documento al quale viene apposta, restando però distinta dal documento.

La firma elettronica avanzata realizza un'unione inscindibile fra il documento e la sottoscrizione e, pertanto, consente non solo l'identificazione del sottoscrittore, ma, essendo stata creata con mezzi sui quali il sottoscrittore ha un controllo esclusivo che gli consentono anche di rilevare se i dati sono stati modificati, realizza un collegamento del documento al firmatario.

La firma elettronica qualificata è una firma avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

La firma elettronica digitale è anch'essa una firma avanzata, basata su un sistema di due chiavi crittografiche, una pubblica e l'altra privata, collegate tra di loro, che consente sia al titolare che al destinatario di verificare la provenienza e la titolarità dei documenti informatici.

La chiave privata, chiamata così in quanto destinata ad essere conosciuta solo dal titolare, consente sia di sottoscrivere il documento, assumendone la paternità, sia di leggere documenti informatici creati da altri soggetti mediante la chiave pubblica.

Per chiave pubblica, invece, si intende quella destinata ad essere resa pubblica attraverso appositi albi tenuti da soggetti chiamati certificatori. La sua funzione è quella di consentire al destinatario di un documento informatico di verificare l'autenticità della firma digitale apposta dal titolare delle chiavi. E' anche utilizzabile per rendere segreto il documento che in tal caso potrà essere letto soltanto dal titolare della chiave privata.

Le due chiavi, pur essendo collegate, possono essere utilizzate congiuntamente o disgiuntamente e garantiscono la riservatezza, l'autenticità e l'integrità del documento informatico.

La segretezza viene garantita "cifrando" in documento con la chiave pubblica del destinatario il quale, essendo in possesso della chiave privata sarà l'unico in grado di decifrare e, quindi, leggere il documento.

L'autenticità viene assicurata mediante la sottoscrizione del documento con la chiave privata da parte

dell'autore.

L'utilizzo di entrambe le chiavi, garantendo sia la segretezza che la provenienza del documento da parte del sottoscrittore, farà si che il documento possa essere considerato integro.

L'art. 21 del CAD[14] attribuisce diverso valore probatorio al documento a seconda della tipologia di firma elettronica apposta. Infatti, al primo comma sancisce il principio secondo cui il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Al comma successivo, però, conferisce rilevanza giuridica alla firma avanzata e alle due particolari

14 Art. 21 *"Documento informativo sottoscritto con firma elettronica: 1. Il documento informativo, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.*

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi non dia prova contraria.

2-bis. Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

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

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

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

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

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie".

categorie di firma qualificata e digitale, stabilendo che, il documento informatico sottoscritto con tali categorie di firme, possiede l'efficacia prevista dall'art. 2702 del codice civile, ossia fa piena prova fino a querela di falso della provenienza delle dichiarazioni da parte del soggetto che l'ha sottoscritto e conferma la presunzione di riconducibilità dell'utilizzo del dispositivo di firma al titolare salvo prova contraria da parte di quest'ultimo[15]. Inoltre, in tutti gli atti e i contratti in cui la legge richiede la forma scritta *ab substantiam* (art. 1350 c.c.) il documento sottoscritto con tali categorie di firma integra il requisito della forma scritta.

4. Le regole tecniche (D.P.C.M. 22 febbraio 2013)

La legge 7 marzo 2005 n. 82, si era limitata a dettare i requisiti generali che una firma elettronica avanzata deve avere stabilendo, all'art. 71, che le regole tecniche previste nel Codice avrebbero dovute essere adottate con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni indicate nel codice, sentita la Conferenza unificata ed il Garante per la protezione dei dati personali, previa acquisizione obbligatoria del parere del CNIPA.

Pertanto, mancando le regole tecniche, le disposizioni del CAD sull'equiparazione del documento informatico con firma digitale alla tradizionale scrittura su carta con firma autografa erano rimaste prive di effetto.

Con la pubblicazione in Gazzetta Ufficiale del D.P.C.M. del 22 febbraio 2013, che ha abrogato il precedente D.P.C.M. del 20 marzo 2009, si è provveduto a colmare il vuoto legislativo emanando le regole tecniche per la generazione, apposizione e verifica della firma elettronica avanzata, qualificata e digitale, per la validazione temporale, nonché per lo sviluppo delle attività dei certificatori qualificati.

Le suddette categorie di firme consentono di scambiare in rete documenti con piena validità legale.

15 Le scritture private previste dall'art. 1350, primo comma, c.c. ai numeri da 1 a 12 (atti che costituiscono, modificano o trasferiscono la proprietà o i diritti reali su beni immobili o mobili registrati ecc.) se posti in essere mediante un documento informatico, devono essere sottoscritte, a pena di nullità, con firma elettronica qualificata o digitale. Quelle previsti al n. 13 del medesimo articolo, invece, possono essere sottoscritte con firma elettronica avanzata, qualificata o digitale.

L'art. 55 del D.P.C.M.[16] stabilisce che la realizzazione di soluzioni di firma elettronica avanzata è libera, non soggetta ad alcuna autorizzazione preventiva e può formare oggetto di attività di impresa. A tal fine distingue due categorie di soggetti che possono offrire il suddetto servizio: a) coloro che lo offrono per motivi istituzionali, societari o commerciali al fine di consentire l'utilizzazione delle firme elettroniche nei rapporti con soggetti terzi; b) coloro che svolgono una vera e propria attività di impresa avente ad oggetto la realizzazione di soluzioni di firma elettronica.

Possono dotarsi di firma elettronica tutte le persone fisiche (cittadini, amministratori, dipendenti pubblici e privati).

Per potersi dotare di firma elettronica è necessario rivolgersi ai c.d. certificatori accreditati, autorizzati dall'Agenzia per l'Italia Digitale (AgID), che sono tenuti a garantire l'identificazione dei soggetti che

16 Art. 55–*Disposizioni generali : 1."La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.*

2. I soggetti che erogano o realizzano soluzioni di firma elettronica avanzata si distinguono in:

a) coloro che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti di cui alla lettera b);

b) coloro che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore dei soggetti di cui alla lettera a).

utilizzano la firma[17]. L'Agenzia esercita poteri di vigilanza sui certificatori.

Il D.P.C.M. prevede, inoltre, che siano rese pubbliche e accessibili le liste dei certificatori revocati e sospesi. I certificati qualificati, su richiesta del titolare, possono essere resi accessibili alla consultazione al pubblico nonché comunicati a terzi , ma al solo fine di verificare la validità delle firme elettroniche qualificate e digitali.

E', infine, riconosciuto a chiunque il diritto di conoscere se sia stato rilasciato un certificato qualificato a proprio nome[18].

17 In proposito, l'art. 15 D.P.C.M. 22 febbraio 2013, rubricato *Informazioni riguardante i certificatori*, prevede che: *"I certificatori che rilasciano al pubblico certificati qualificati ai sensi del Codice forniscono all'Agenzia le seguenti informazioni e documenti a loro relativi:*

a) *dati anagrafici ovvero denominazione o ragione sociale;*
b) *residenza ovvero sede legale;*
c) *sedi operative;*
d) *rappresentanza legale;*
e) *certificati delle chiavi di certificazione;*
f) *piano per la sicurezza di cui all'art. 35;*
g) *manuale operativo di cui all'art. 40;*
h) *relazione sulla struttura organizzativa;*
i) *copia di una polizza assicurativa a copertura dei rischi dell'attività e dei danni causati ai terzi.*

2. L'Agenzia rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), e), g) al fine di rendere pubbliche le informazioni che individuano il certificatore qualificato. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge".

Il successivo art. 16, *Comunicazione tra certificatore e l'Agenzia*, stabilisce che: *"1. I certificatori che rilasciano al pubblico certificati qualificati comunicano all'Agenzia la casella di posta elettronica certificata da utilizzare per realizzare un sistema di comunicazione attraverso il quale scambiare le informazioni previste dal presente decreto.*
2. L'Agenzia rende disponibile sul proprio sito internet l'indirizzo delle propria casella di posta elettronica certificata".

18 Art. 34 *Accesso del pubblico ai certificati: "1. Le liste dei certificati revocati e sospesi sono rese pubbliche.*

2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione al pubblico nonché comunicati a terzi, al fine di verificare le firme digitali, esclusivamente nei casi consentiti dal titolare del certificato e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.

3. Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione al pubblico, sono utilizzabili da chi li consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità delle firme elettroniche qualificate e digitali.

4. Chiunque ha diritto di conoscere se a proprio nome sia stato rilasciato un certificato qualificato. Le modalità per ottenere l'informazione di cui al primo periodo sono definite con il provvedimento di cui all'art. 42, comma 10, del presente decreto".

5. Il disconoscimento del documento sottoscritto con firma elettronica

L'equiparazione operata dal legislatore tra il documento cartaceo e quello informatico, con conseguente applicazione delle regole in materia di efficacia probatoria, ha acceso un vivace dibattito in dottrina sulla possibilità di disconoscere il documento sottoscritto con firma elettronica applicando le stesse regole previste per il disconoscimento di scritture private cartacee sottoscritte con firma autografa.

La scrittura privata, come è noto, a differenza dell'atto pubblico è creata dallo stesso autore dell'atto e, pertanto, deve essere sottoscritta. Se priva di sottoscrizione non può nemmeno essere considerata scrittura privata. La disciplina in materia di scrittura privata è contenuta nel libro VI del codice civile relativo alla tutela dei diritti ed in particolare nel capo II che si occupa delle prove.

L'art. 2702 c.c. regola l'efficacia probatoria della scrittura privata stabilendo che:

"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".

Alla suddetta norma si ricollegano le disposizioni del codice di procedura civile contenute negli artt. 215 in tema di riconoscimento tacito della scrittura privata e 216 in materia di verificazione[19].

Elementi costitutivi della fattispecie sono, pertanto, il riconoscimento da parte del sottoscrittore o, in alternativa, l'autentica da parte di un notaio o di un pubblico ufficiale a ciò autorizzato, la contumacia

19 *Art. 215 c.p.c.- Riconoscimento tacito della scrittura privata: "La scrittura privata prodotta in giudizio si ha per riconosciuta:*
1) se la parte alla quale la scrittura è attribuita o contro la quale è prodotta è contumace salva la disposizione dell'articolo 293 terzo comma;
2) se la parte comparsa non la riconosce o non dichiara di non conoscerla nella prima udienza o nella prima risposta successiva alla produzione.
Quando nei casi ammessi dalla legge, la scrittura è prodotta in copia autentica, il giudice istruttore può concedere un termine per deliberare alla parte che ne fa istanza nei modi di cui al numero 2.
Art. 216 – Istanza di verificazione: "La parte che intende valersi della scrittura disconosciuta deve chiederne la verificazione, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire di comparazione.
L'istanza di verificazione può anche proporsi in via principale con citazione, quando la parte dimostra di avervi interesse; ma se il convenuto riconosce la scrittura le spese sono posta a carico dell'attore.

del sottoscrittore, il disconoscimento fuori termine (art. 215 n. 1 e 2 c.p.c.), la verificazione giudiziaria.

Dal combinato disposto delle tre norme si desume che la semplice sottoscrizione non è di per se sola sufficiente a far conseguire alla scrittura privata efficacia di prova legale se non concorrono altri requisiti, come il riconoscimento espresso o tacito, l'autenticazione o l'esito positivo della verifica giudiziaria.

Il principio secondo cui il documento informatico, sottoscritto con firma elettronica, aveva efficacia di scrittura privata ai sensi dell'art. 2702 del codice civile era stato già affermato dalla legislazione previgente all'entrata in vigore del CAD. Era sorto, pertanto, il problema se anche la scrittura privata informatica, avesse bisogno della ricorrenza dei suddetti requisiti o se, per le caratteristiche tecniche di tale tipo di firma, acquistasse automaticamente valore di prova legale. Il generico rinvio operato dal legislatore dell'epoca alla norma civilistica senza alcun riferimento agli articoli del codice di procedura che ne integrano la disciplina aveva alimentato i dubbi della dottrina sulla compatibilità della firma elettronica con le caratteristiche del disconoscimento.

Approfondiamo, tuttavia, preventivamente una questione che si è posta con riferimento alla conservazione del documento elettronico stampato e alla sua validità probatoria.

L'art. 23 del Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.), riconosce alle copie analogiche di documenti informatici (es. la stampa di un certificato, un contratto, ecc.) la stessa efficacia probatoria dell'originale informatico da cui sono tratti se la loro conformità non viene espressamente disconosciuta (in giudizio). Diverso è il caso in cui la conformità all'originare informatico, in tutte le sue componenti, sia attestata da un pubblico ufficiale autorizzato. In questo caso, infatti, per negare alla copia analogica di documento informatico la stessa efficacia probatoria del documento sorgente si rende necessaria la querela di falso.

Questo regime, di carattere generale, incontra alcune deroghe rispetto alle copie analogiche di documenti amministrativi informatici. In primo luogo l'art. 23-ter del CAD prevede che sulle copie analogiche di documenti amministrativi informatici possa essere apposto un contrassegno a stampa (detto anche timbro digitale o glifo) che consente di accertare la corrispondenza tra le copie analogiche stesse e l'originale informatico (in esso deve essere codificato, infatti, il documento informatico o le informazioni necessarie a verificarne la corrispondenza all'originale in formato digitale). La verifica

avviene grazie ad appositi software che leggono le informazioni contenute nel timbro digitale. I software necessari per l'attività di verifica devono essere gratuiti e messi liberamente a disposizione da parte delle amministrazioni.

Inoltre, il c.d. Decreto crescita 2.0 – Decreto Legge 18 Ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221) ha previsto un regime semplificato per l'invio, cittadini sprovvisti di domicilio digitale, di comunicazioni diverse dai certificati che dovranno essere utilizzati nei rapporti tra privati. In questo caso l'amministrazione può inviare al cittadino una copia analogica dei documenti stessi, sottoscritta con firma autografa sostituita a mezzo stampa, conformemente alle previsioni di legge (Decreto Legislativo 12 dicembre 1993, n. 39). L'amministrazione che invia copia cartacea della comunicazione redatta in originale informatico dovrà apporre una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso l'amministrazione.

5.1 Teorie favorevoli al disconoscimento della firma elettronica

Una parte della dottrina[20], applicando alla lettera le disposizioni civilistiche riteneva che anche per il documento informatico sottoscritto con firma elettronica, fosse necessario il riconoscimento della firma e, pertanto, ne ammetteva la possibilità di disconoscimento; altri[21], partendo dal principio che il documento sottoscritto con firma elettronica avesse valore di prova legale fino a querela di falso, escludeva la possibilità del disconoscimento.

I sostenitori della prima teoria ritenevano possibile il disconoscimento della firma elettronica in

20 Ferrari – La nuova disciplina del documento informatico in Rivista di diritto processuale 1999, pp. 129-162; Reggiani – Forma e firma digitale: struttura e valore probatorio del documento informatico, in Documenti di giustizia 1998, pp. 1584-1600; De Santis – Tipologia e diffusione del documento informatico. Pregresse difficoltà di un suo inquadramento normativo, in Corriere Giuridico 1998, pp. 383-396; Piccoli Zanolini – Il documento elettronico e la firma digitale, in I problemi giuridici di internet, pp. 57104; Alberti – Sul documento informatico e sulla firma digitale, in Giustizia civile 1998, pp. 267-310; Orlandi F.– Il regolamento sul documento elettronico: profili ed effetti, in Rivista del diritto commerciale e del diritto generale delle obbligazioni, 1998, pp. 743-772.

21 Bianca –I contratti digitali, in Studiumiuris, 1998, pp. 1035-1040; Finocchiaro – Documento informatico e firma digitale, in Contratto e impresa 1998, pp. 956-987; Gentili – Documento informatico e tutela dell'affidamento, in Rivista di diritto civile, 1998, pp. 163-179; Tripodi Gasparini – Firma digitale e documento informatico. Una disciplina unica per l'ambito pubblico e privato, Buffetti editore, 1998; Graziosi – Pregresse ad una teoria probatoria del documento informatico, in Rivista trimestrale di diritto e procedura civile, 1998, pp. 481-529; Delfini – Il D.P.R. 513 e il contratto telematico, in I contratti, 1998, pp. 293-305.

quanto non esisteva alcuna norma che autorizzasse a sostenere il contrario. Inoltre, sostenevano che la firma elettronica non potesse essere equiparata ad una sottoscrizione legalmente riconosciuta e, pertanto, in mancanza di riconoscimento espresso o tacito o di autenticazione, poteva essere disconosciuta e successivamente sottoposta a procedimento di verificazione. In altri termini, sarebbe stato impensabile considerare il documento informatico sottoscritto con firma elettronica alla pari di una scrittura privata autenticata, rendendo superflui ulteriori controlli, come se il titolare della firma fosse munito di poteri di autentica come un pubblico ufficiale. Senza considerare, poi, che il pubblico ufficiale in sede di autentica non si limita ad attestare che la firma è stata opposta in sua presenza, ma accerta anche l'identità del sottoscrittore, nonché la coerenza dell'atto con l'ordinamento giuridico.

I sostenitori della teoria che ammetteva il disconoscimento della firma elettronica facevano, inoltre, riferimento all'art. 24 del D.P.R. 28 dicembre 2000, n. 445[22] che prevedeva l'autenticazione della firma digitale da parte di un notaio o di un pubblico ufficiale autorizzato, consistente nell'attestazione che la firma era stata apposta in loro presenza dal titolare, previo accertamento della sua identità personale e della validità della chiave utilizzata. L'anzidetta norma richiedeva anche un ulteriore controllo sulla rispondenza dell'atto alla volontà della parte. La presenza dell'art. 24, per questi autori, dimostrava in modo non equivoco come la firma elettronica di per se non fosse idonea a conferire valore di prova legale alla scrittura privata e che potesse, quindi, essere disconosciuta dal titolare e sottoposta alla procedura di verificazione.

Qualche autore[23] aveva anche ritenuto che l'onere di disconoscere la firma elettronica, onde evitare la presunzione ex art. 215 n. 2 c.p.c., fosse giustificato dal fatto che la procedura di certificazione non garantiva l'autenticità della firma essendo elevato il rischio di frodi derivante dall'uso improprio delle chiavi asimmetriche. Qualcun altro[24] si era espresso a favore dell'applicazione analogica delle norme contenute nel codice di procedura civile al documento informativo partendo dal presupposto che la *ratio* della verificazione sta nel fatto che la scrittura privata, essendo stata precostituita dalle parti prima del processo, ha una minor forza di convincimento rispetto alle altre prove liberamente valutabili dal giudice.

22 Abrogato dal D.lgs. 7 marzo 2005, n. 82 (CAD).

23 Fedele – op.cit..

24 De Santis – op. cit..

La suddetta corrente dottrinaria, dopo aver affermato la possibilità di disconoscere la firma elettronica aveva anche affrontato il problema se i principi e le norme che regolano il disconoscimento della scrittura privata fossero automaticamente applicabili al documento informatico o se, la diversità del supporto richiedesse aggiustamenti e modifiche. Le soluzioni proposte possono sinteticamente essere raggruppate in tre tesi.

Secondo la prima tesi le disposizioni in materia di disconoscimento della firma su supporto cartaceo potevano essere automaticamente applicate anche ai documenti informatici sottoscritti con firma elettronica. Di conseguenza, un soggetto contro il quale fosse stato prodotto un documento informatico avrebbe avuto soltanto l'onere di disconoscerlo gravando sull'altra parte la prova dell'autenticità della firma. La suddetta tesi non ha avuto seguito in dottrina in quanto consentiva al titolare della firma digitale di disconoscerla senza fornire prove al riguardo[25], addossando all'altra parte l'onere di provare l'autenticità della firma. Inoltre, non essendo possibile far ricorso a scritture di comparazione, trattandosi di scrittura informatica, sarebbe stato anche impossibile per la parte che produceva il documento in giudizio fornire la prova dell'autenticità della firma.

La seconda tesi[26] sosteneva che il soggetto che produceva un documento digitale, di fronte al disconoscimento della firma, poteva chiedere che venisse effettuata una verifica tecnica per accertare la corrispondenza tra la chiave pubblica e quella privata, senza che l'altra parte potesse dimostrare il contrario nel corso della verifica. In questo modo non sarebbe stato precluso il disconoscimento, ma si sarebbe reso più difficile contestare l'autenticità. Qualche autore[27] aveva anche proposto una modifica dei mezzi di prova per poter applicare la disciplina del disconoscimento anche al documento informatico, nel senso che, sarebbe stato sufficiente provare l'esistenza di un certificato valido per collegare la chiave al suo titolare. In senso contrario[28]era stato opposto che, così operando, il disconoscimento e la successiva verificazione avrebbero perso di significato riducendosi ad una mera verifica tecnica della firma elettronica.

25 Gentili op. cit..
26 Orlandi M. – op. cit..
27 Fedeli – op. cit..
28 Zagami – op.cit..

La terza tesi[29] si concentrava sul giudizio di verificazione sostenendo che, a seguito della verifica tecnica sulla firma elettronica, avente ad oggetto la corrispondenza tra la chiave privata e la chiave pubblica e l'esistenza di un valido certificato, il soggetto che sarebbe risultato titolare della chiave privata utilizzata per sottoscrivere l'atto avrebbe avuto l'onere di dimostrare di non essere l'autore della firma. In tal caso si sarebbe avuta un'inversione dell'onere della prova addossandola non più al soggetto che presenta il documento in giudizio, ma a chi ne contestava l'autenticità che avrebbe dovuto dimostrare l'uso illecito della propria chiavetta.

E' stato obbiettato che[30], adottando la tesi in precedenza opposta, si sarebbe ampliato troppo l'oggetto del giudizio di verificazione rendendo praticamente inutile la querela di falso ed, inoltre, si sarebbe travisato lo scopo della verifica che ha per oggetto l'attribuzione della firma ad un determinato soggetto e non la dimostrazione della falsità.

5.2 Teorie contrarie al disconoscimento della firma elettronica

Secondo un'altra corrente di pensiero il disconoscimento e la successiva procedura di verifica sarebbero incompatibili con il sistema della firma elettronica. E' stato innanzitutto contestato il punto di partenza delle precedenti teorie secondo le quali la mancanza di un riferimento normativo alla procedura di disconoscimento non ne escludeva l'applicazione[31].

Era stato, infatti, precisato che, il richiamo contenuto nell'art. 10 D.P.R. 445/2000[32], all'epoca vigente, all'art. 2702 c.c. andava riferito solo all'efficacia probatoria, in quanto, se l'intenzione del legislatore fosse stata quella richiamare tutta la disciplina sul disconoscimento, le formule usate avrebbero dovuto essere diverse, senza contare, poi, che, mentre con la sottoscrizione manuale si instaurava un rapporto personale tra il firmatario e l'atto, con quella elettronica viene a crearsi una relazione tra chiavi asimmetriche e titolare della firma. In altri termini il particolare tipo di rapporto che intercorre tra la firma elettronica e il suo autore non consentirebbe al titolare della chiave di negare la provenienza della

29 Reggiani, Orlandi F. Zagami, Fedeli - op. cit.

30 V. Problematiche sul disconoscimento della firma digitale, in Jei – Jus e internet, pp.4 e segg..

31 Graziosi – op. cit.

32 Abrogato dal D.lgs. 7 marzo 2005, n. 82.

firma[33]. Con l'utilizzo della firma grafica si instaura un rapporto soggettivo, mentre in quella elettronica una relazione oggettiva e, pertanto, in sede di verifica si può solo stabilire che quella firma proviene da una determinata chiave attribuita ad un determinato soggetto. Qualche autore[34] ha precisato che la firma elettronica non è in grado di fornire la prova della paternità dell'atto, ma solo l'identità del titolare della chiave.

Altri[35] hanno posto in rilievo che dubbi sulla paternità dell'atto avrebbero potuto sorgere solo se il legislatore non avesse previsto un sistema di certificazione delle chiavi. La previgente normativa, come del resto anche quella attuale, prevedeva una procedura di certificazione che, garantendo la corrispondenza tra un soggetto, la chiave pubblica e quella privata rendeva di fatto autentica la firma apposta fino alla scadenza del certificato. Inoltre, fra gli obblighi del certificatore era previsto anche quello di identificare con certezza la persona che richiedeva la certificazione. Del resto non mancavano riferimenti legislativi al soggetto a cui imputare la firma elettronica, identificato nel titolare della coppia di chiavi: quella privata per sottoscrivere e quella pubblica per verificare la firma apposta. Pertanto, secondo i sostenitori di questa corrente dottrinaria, vi sarebbe stata una presunzione assoluta di riferibilità della firma al titolare della chiave privata, incompatibile con la procedura di disconoscimento della sottoscrizione prevista per la firma su supporto cartaceo. In conclusione, non potendo la firma elettronica essere riferita a soggetti diversi dal titolare della coppia di chiavi asimmetriche, certificate, la firma doveva considerarsi autenticata e, pertanto, non ci sarebbe stato bisogno del verificarsi delle condizioni a cui fa riferimento l'art. 2702 c.c. per acquistare l'efficacia di prova legale.

I sostenitori della suddetta tesi si erano anche posti il problema che, accettando le conclusioni proposte, sembrava superflua la disposizione[36] sull'autenticazione della firma elettronica,avendo quest'ultima già acquisito valore di prova legale. Il dubbio era stato risolto[37] sostenendo che la disposizione all'epoca in vigore conservava la propria ragion d'essere in quanto non si limitava a prevedere che la firma elettronica fosse apposta dal titolare della chiave in presenza di un notaio o di un pubblico ufficiale appositamente autorizzato, ma richiedeva anche ulteriori adempimenti consistenti nella verifica della

33 In tal senso cfr. Bianca – op. cit..

34 Orlandi – op. cit..

35 Gasparini, Tripoldi – op.cit..

36 Art. 24 D.P.R. 445/2000, abrogato dal D.P.R. 7 marzo 2005, n. 82 (CAD).

37 Gentili – op. cit..

corrispondenza della dichiarazione riportata nella scrittura alla reale volontà del dichiarante nonché la compatibilità delle affermazioni con i principi generale dell'ordinamento giuridico.

5.3 Soluzione adottata dal CAD

Gli approfondimenti dottrinari hanno avuto l'indiscusso merito di sollecitare il legislatore ad adottare una disciplina più chiara. L'art. 21, comma 2,del CAD, nel testo attualmente in vigore, espressamente prevede che: *"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscono l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria".*

Dall'interpretazione della formula legislativa si evince che l'utilizzo della firma elettronica determina una presunzione *juris tantum* di paternità del documento informatico[38] da parte di colui che appare come sottoscrittore e che, tra l'altro, è anche l'unico soggetto legittimato a contestarne l'autenticità.

5.4 Compatibilità della firma elettronica con la querela di falso

Esaminate le problematiche relative all'applicazione delle norme civilistiche sul disconoscimento della firma su supporto cartaceo ai documenti informatici, resta ora da esaminare l'applicabilità dell'altro strumento processuale: la querela di falso.

La dottrina dominante[39] ritiene che il suddetto strumento, considerate le caratteristiche diverse rispetto al disconoscimento, possa essere applicato alla firma elettronica distinguendo due ipotesi: una relativa alla firma elettronica non autenticata, l'altra a quella autenticata.

Nella prima ipotesi l'esperibilità della querela di falso sarebbe giustificata in quanto la verifica tecnica individua solo una relazione oggettiva tra il titolare delle chiavi e la firma elettronica, ma non è in grado di escludere l'utilizzazione delle chiavi da parte di altri soggetti non autorizzati. Per ottenere questa certezza si rendono necessari ulteriori e più approfonditi accertamenti aventi ad oggetto non la falsità

38 In tal senso cfr. Minussi – Valore legale della firma digitale, in WikiJus, pp.1-9.

39 Finocchiaro, Zagami, Graziosi, Gentili, De Santis, Orlandi M., Reggiani – op. cit..

della firma, ma l'illecito utilizzo da parte di altri. Inoltre, non essendo ammissibile il disconoscimento, la querela di falso rimarrebbe l'unico strumento a disposizione del titolare della firma elettronica per dimostrare l'uso abusivo delle chiavi.

Oggetto della querela, nel giudizio civile, sarà quello di dimostrare che il titolare della firma elettronica non l'ha realmente apposta, in quanto, ad esempio, ha subito una sottrazione della *smart card* e del codice identificativo. I mezzi di prova sono liberi anche se in pratica sarà molto difficile convincere il giudice a dichiarare la falsità della firma specialmente per i contratti conclusi mediante l'utilizzo della rete internet. Il raggiungimento della prova della sottrazione potrà portare alla dichiarazione di falsità dell'atto, ma non escluderà conseguenza in tema di risarcimento dei danni a carico dell'apparente sottoscrittore nei casi in cui risulti che non abbia adottato le cautele necessarie per custodire il dispositivo di firma.

Per i sostenitori di questa teoria, dunque, la querela rimane l'unico strumento per dimostrare la falsità della firma apposta in calce all'atto, mentre per i sostenitori del disconoscimento, la querela sarebbe un rimedio più ampio che si verrebbe ad aggiungere alla procedura di verificazione.

Per quanto riguarda la seconda ipotesi, ossia la proposizione della querela di falso contro un documento con firma elettronica autenticata, l'oggetto della verifica è più ristretto non essendo possibile contestare né l'identità del soggetto né l'apposizione della firma. E' praticamente limitata alle ipotesi di falso ideologico da parte del notaio o del pubblico ufficiale e costituisce per il soggetto che agisce in giudizio una vera e propria *probatio diabolica*.