GIOVANNI BUONOMO-ANIELLO MERONE

LA SCRITTURA PRIVATA INFORMATICA: FIRME ELETTRONICHE, VALORE PROBATORIO E DISCONOSCIMENTO IN GIUDIZIO [ALLA LUCE DELLE MODIFICHE INTRODOTTE DALLA L. 221/2012]

SOMMARIO: 1. Premessa. — 2. Il quadro normativo. — 3. Documento e scrittura informatica. — 4. Le diverse tipologie di firme elettroniche. — 5. Efficacia sostanziale e valore probatorio delle scritture informatiche. — 6. Disconoscimento e verificazione della scrittura privata informatica.

1. Premessa.

Con le modifiche introdotte dalla legge 17 dicembre 2012, n. 221, l'articolo 21 del codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82) — dedicato, com'è noto, alla disciplina del valore probatorio e di scrittura privata dei documenti informatici — è stato sostanzialmente modificato per la terza volta nell'arco di sette anni.

Avendo ad oggetto innovazioni radicali in materie così rilevanti (destinate, secondo l'intento del legislatore, a cambiare il rapporto tra Stato e cittadini[1]) il « codice » avrebbe invero meritato un più meditato periodo di attesa per favorire il consolidamento delle opinioni dottrinali e l'evolu-

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

** Il presente lavoro è stato realizzato nell'ambito della ricerca « La regolamentazione giuridica delle Tecnologie dell'Informazione e della Comunicazione (TIC) quale strumento di potenziamento delle società inclusive, innovative e sicure » finanziata dal Dipartimento di Scienze Umane dell'Università Europea di Roma e dal MIUR (PRIN 2010-2011).

[1] Non a caso la sezione seconda del codice è enfaticamente dedicata ai *diritti dei cittadini e delle imprese nei confronti della pubblica amministrazione* e l'art. 10 della legge-delega 29 luglio 2003, n. 229, individua tra le sue finalità quella di « ... garantire la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici e di assicurare ai cittadini e alle imprese l'accesso a tali servizi secondo il criterio della massima semplificazione degli strumenti e delle procedure necessari e nel rispetto dei rincipi di eguaglianza, non discriminazione e della normativa sulla riservatezza dei dati personali ». Sul punto, N. Lugaresi, *Codice dell'amministrazione digitale e rapporti tra cittadino e Pubblica Amministrazione*, in *Giustizia amministrativa*, 2006, fasc. 2, p. 460 ss.; sui mutamenti indotti dall'introduzione delle tecnologie dell'informazione nella pubblica amministrazione, P. Costanzo, *Nuove tecnologie e « forma » dell'amministrazione*, in P. Costanzo, G. Deminico, R. Zaccaria (a cura di), *I tre codici della società dell'informazione: amministrazione digitale, comunicazioni elettroniche, contenuti audiovisivi*, Torino, 2006, p. 3 ss.; sullo stesso tema, E. D'Orlando, *Profili costituzionali dell'amministrazione digitale*, in *Dir. inf. e informatica*, 2011, 2, p. 213 ss.

zione della giurisprudenza, in luogo di questo primato di modificazioni, integrazioni, aggiunte e cancellazioni, che sembrano celare, in taluni casi, un tardivo ripensamento del legislatore.

Eppure l'Italia è stata uno dei primi Paesi al mondo ad equiparare, agli effetti giuridici, i documenti informatici muniti di firma digitale ai documenti formati su supporto cartaceo[2]; con ciò accogliendo (e, per certi versi, anticipando) la spinta, favorita da una molteplicità di fattori economici, tecnologici e politici che caratterizzarono la fine degli anni Novanta, all'uso delle tecnologie dell'informazione come strumento per il recupero di efficienza e di razionalità nella pubblica amministrazione.

Il codice dell'amministrazione digitale del 2005 avrebbe dovuto raccogliere ed organizzare razionalmente le numerose norme che, in circa un decennio, si erano venute affastellando sulla disciplina dello scambio di informazioni, per via telematica, tra pubbliche amministrazioni, della realizzazione di una infrastruttura tecnologica di rete nazionale, dello sviluppo e del « riuso » dei sistemi informatici delle pubbliche amministrazioni centrali e locali, della formazione e dell'archiviazione dei documenti su supporto informatico. Tuttavia, come avvenuto per gli altri « codici » adottati in forza della legge di semplificazione del 2001[3], l'intento del legislatore si è spinto ben al di là del semplice riordino delle norme di settore, giungendo sino a toccare la complessa materia del valore probatorio dei documenti informatici e le norme di recepimento della direttiva comunitaria sulle firme elettroniche[4].

[2] Il Libro Bianco della Commissione europea [COM(93)700], pubblicato nel dicembre del 1993 sotto la presidenza di Jacques Delors, individuava nelle tecnologie dell'informazione e della comunicazione (ICT) il settore dell'economia a maggior tasso di crescita, nell'ottica di creare 15 milioni di posti di lavoro in Europa entro l'anno 2000 attraverso uno « sviluppo sostenibile » dell'economia, basato su interventi compatibili con le caratteristiche della società europea (riduzione della spesa pubblica, aumento degli investimenti produttivi, riduzione della tassazione del lavoro e del costo del denaro). In generale, M. D'ANTONA, *Armonizzazione del diritto del lavoro e federalismo nell'Unione europea*, in *Rivista trimestrale di diritto e procedura civile*, 1994, p. 695 ss., sp. 713-715; P. RUGGERO, *Il Libro bianco: principali indicazioni e possibili implicazioni economiche*, in *Rivista giuridica del lavoro e della previdenza sociale*, 1994, p. 87 ss.; G. ARRIGO-A. SOLUSTRI, *Prime considerazioni sul Libro bianco*, in *Rivista giuridica del lavoro e della previdenza sociale*, 1994, p. 98 ss. Il tema venne poi sviluppato organicamente nel famoso « Rapporto Bangemann » pubblicato nel 1994 all'esito del lavoro di un gruppo di esperti di alto livello, costituito su mandato del Consiglio e presieduto dal commissario europeo Martin Bangemann, ove si faceva cenno, per la prima volta, alle firme elettroniche che avrebbero dovuto sostituire le firme autografe su documenti formati su supporti informatici e destinati a sostituire completamente i supporti cartacei (anche nell'impiego, in caso di controversie, come prova in giudizio). Sul tema, G. SANTANIELLO, *Prospettive legislative concernenti la multimedialità*, ne *Il diritto dell'economia*, 1995, p. 631 ss.

[3] Secondo N. IRTI, *Codici di settore e compimento della decodificazione*, in M.A. SANDULLI, *Codificazione, semplificazione e qualità della regolazione*, Milano, 2005, p. 7 e p. 19 ss., i codici di settore costituirebbero una manifestazione del processo di decodificazione che, seguendo il declino della tradizionale forma storica del codice, affida rilevanti materie a sedi esterne. I codici di settore, dunque, costituirebbero non già leggi speciali, ma « leggi specializzate: di quella specializzazione determinata dalla tecno-economia... » che, per la loro intima connessione con le esigenze dello sviluppo tecnico ed economico, darebbero vita ad un corpo di « norme instabili » definito come « diritto frazionario ».

[4] Sul tema, *amplius* in M. PIETRANGELO, *La società dell'informazione tra realtà e norma*, Milano, 2007, p. 86 ss.; F. DELFINI, *L'evoluzione normativa della disciplina del documento informatico: dal D.P.R. 513/1997 al Codice dell'amministrazione*

2. Il quadro normativo.

Per dare valore legale ai documenti destinati a circolare nell'ambito della Rete unitaria delle pubbliche amministrazioni (la RUPA[5]) l'Italia ha introdotto nell'ordinamento, sin dal 1997 (con l'art. 15, comma 2, della legge n. 59), il fondamentale principio di equivalenza, secondo cui « gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge ».

Si tratta di una norma che, formalmente in vigore da quindici anni, non ha, in realtà, goduto di alcuna stabilità applicativa.

Il problema è noto: le disposizioni regolamentari destinate a dare attuazione al principio di legge, ancorché emanate tempestivamente, hanno subito continui interventi correttivi che denunciano, più che l'incertezza del legislatore di fronte alla novità della materia, un evidente condizionamento del diritto, nelle materie « informatiche », ad opera della tecnica[6].

In un primo momento, infatti, i « criteri e modalità di applicazione » del principio di equivalenza furono stabiliti dal D.P.R. n. 513 del 1997 che (emanato a distanza di pochi mesi dalla legge n. 59) prevedeva, all'art. 10, comma 2, « l'apposizione o l'associazione della firma digitale al documento informatico » quale strumento equivalente alla sottoscrizione autografa dei documenti scritti su supporto cartaceo e attribuiva, *ex* art. 5, al « documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10... efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile »[7].

digitale, in *Riv. dir. priv.*, 2005, p. 531 ss. In generale, per un commento organico del codice dell'amministrazione digitale, si veda G. Duni, voce: *Amministrazione digitale*, in *Enc. dir. - Annali [Accertamento - Tutela]*, I, Milano, 2007, p. 13 ss.; G. Cassano-C. Giurdanella, *Il codice della pubblica amministrazione digitale*, Milano, 2005.

[5] Nel sistema della RUPA, oggi sostituito dal Sistema pubblico di connettività, le reti informatiche delle singole amministrazioni avrebbero dovuto confluire in un sistema integrato « unitario », accessibile per via telematica da ciascuno dei soggetti « federati », pur consentendo alla struttura informativa di ogni amministrazione pubblica manteneva la propria autonomia di gestione. Da ciò la definizione della Rete unitaria come « rete di reti », in cui ogni soggetto partecipante poteva realizzare e gestire il proprio sistema informativo, ma era tenuto ad osservare le regole tecniche comuni emanate dall'Autorità per l'informatica nella pubblica amministrazione (AIPA) per potersi connettere alla rete informatica delle altre amministrazioni e scambiare informazioni. Sul tema vedi ampliamente A. Contaldo *Le reti della Pubblica Amministrazione e il progetto della Rete unitaria della Pubblica Amministrazione (RUPA)*, in *Il Foro amm.-C.d.S.*, 2004, p. 2371 ss.; Id., *La sicurezza della rete: lineamenti giuridici su una innovazione tecnologica al servizio della P.A.*, in *Riv. amm. Rep. it.*, 2003, I, p. 707 ss.; M. Zambuco, *La comunicazione in Internet e gli ambiti operativi delle reti amministrative pubbliche centrali e periferiche*, in - *Riv. trim. scie. amm.*, 2004, p. 107 ss.

[6] Secondo G. Finocchiaro, *Riflessioni su diritto e tecnica*, in *Dir. inf. e inform.*, 2012, p. 831 ss. nelle materie della sicurezza informatica e della firma digitale « l'informatica condiziona sin dall'origine, definendone i termini, il lavoro del giurista ». L'A. si richiama agli studi di J.L. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, p. 553 ss., per sostenere che il diritto positivo si affida sempre più frequentemente alla tecnica per difendere i diritti (come nel caso delle misure tecnologiche per la protezione del diritto d'autore).

[7] Si veda M. Miccoli, sub *art. 1*, in

Col D.P.C.M. 8 febbraio 1999, contenente le « regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici » si portò a definitivo compimento il quadro normativo che introduceva nell'ordinamento (disciplinandolo in tre fasi, attraverso la legge fondamentale, il regolamento e le regole tecniche) un sistema basato sulla piena equiparazione del documento informatico, munito di firma digitale, alla tradizionale scrittura privata formata e sottoscritta sul supporto cartaceo[8].

Il regolamento del 1997 fu successivamente abrogato dal D.P.R. 28 dicembre 2000, n. 445 (testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), nel quale confluirono le norme sul documento e sulla firma digitale[9], senza smarrire la coerenza del nuovo sistema e la fondamentale equiparazione summenzionata.

Profondi cambiamenti, invece, furono innescati dalla direttiva comunitaria 1999/93/CE.

Preceduta da un difficile negoziato politico e da un aspro dibattito tecnico, la direttiva muoveva dalla necessità di stabilire una disciplina sovranazionale che riconducesse ad un quadro normativo unitario le diverse discipline adottate dai singoli Stati dell'Unione[10], al fine di agevolare l'uso

Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici, Commentario del D.P.R. 10 novembre 1997, n. 513, a cura di C.M. Bianca, R. Clarizia, V. Franceschelli, F. Gallo, L.V. Moscarini, A. Pace e S. Patti, in *Nuove leggi civ. comm.*, 2000, p. 633 ss.; S. Patti, *L'efficacia probatoria del documento informatico*, in *Riv. dir. proc.*, 2000, p. 60 ss.; F. De Santis, *La disciplina normativa del documento informatico*, in *Corriere giur.*, 1998, p. 379 ss.; G. Finocchiaro, *Documento informatico e firma digitale*, in *Contratto e impresa*, 1998, p. 956 ss.; M. Miccoli, *Documento e commercio telematico - guida al regolamento italiano (D.P.R. n. 513/1997)*, Milano, 1998.

[8] Diffusamente e con ampi richiami critici, vedi, R. Zagami, *Firma digitale e sicurezza giuridica*, Padova, 2000, sp. 25 ss.

[9] L'art. 10 del testo unico del 2000, in vigore dal 7 marzo 2001 sino al 1 luglio 2003, disponeva che « Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche [...] soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del codice civile [...] 3. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del Codice civile. 4. Il documento informatico redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del Codice civile e da ogni altra analoga disposizione legislativa o regolamentare. L'art. 23, dedicato alla firma digitale, disponeva che « 1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale. 2. - L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo. ». Per approfondimenti, si veda G. Fares, *Il Testo Unico sulla Documentazione Amministrativa*, in *Studium iuris*, 2002, p. 172 ss.; F. Patroni Griffi, *Un'introduzione al testo unico sulla documentazione amministrativa: metologia e procedure*, in *Comuni d'Italia*, 2001, p. 1023 ss.

[10] A seguire l'esempio dell'Italia erano state, in particolare: la Spagna, che con la legge 30 dicembre 1997, n. 66 aveva introdotto, per la pubblica amministrazione, un sistema di autenticazione informatica per le procedure amministrative, sotto il controllo della *Fábrica Nacional de Moneda y Timbre*; la Germania, che nel 1997 aveva modificato la propria normativa in materia di telecomunicazioni disciplinando l'uso della firma digitale nell'ambito di un'infrastruttura a chiavi pubbliche di cifratura (in sostanza adottando lo stesso schema italiano) sotto il controllo dell'Agenzia federale per la sicurezza informatica (*Bundesamt fur Sicherheit in der Informationstechnik*); l'Austria, il cui Consiglio dei Ministri aveva adottato, il 9 luglio 1998, una direttiva di carattere generale che prevedeva regole giuridiche per l'uso

delle firme elettroniche per la sottoscrizione dei documenti informatici e « contribuire al loro riconoscimento giuridico » in ambito europeo[11]. Per questo, tutte le disposizioni del testo comunitario erano (e restano tuttora) ispirate al principio di neutralità tecnologica, che vieta al legislatore nazionale di condizionare, anche indirettamente, attraverso il riferimento a standard tecnologici adottati da specifici prodotti, la libera circolazione dei prodotti e dei servizi utilizzabili per le firme elettroniche.

In Italia ed in Germania, dove i regolamenti adottati prima dell'emanazione della direttiva facevano esclusivo riferimento al sistema di cifratura a chiave pubblica, si rese allora necessario rivedere tutte le disposizioni che — di fatto — ammettevano per la firma di un documento informatico soltanto prodotti software riferibili ad una infrastruttura di distribuzione delle chiavi pubbliche nell'ambito di sistemi di firma digitale[12].

della firma digitale; il Belgio che, nello stesso periodo (il 12 giugno 1998) con delibera del Consiglio Federale dei Ministri aveva approvato un disegno di legge sulla firma digitale che adottava lo stesso sistema a chiavi asimmetriche di cifratura previsto dalla legislazione italiana e tedesca, istituendo autorità qualificate di certificazione per il rilascio di certificazioni sulle chiavi pubbliche e prevedendo una sorta di omologazione riferita al possesso dei requisiti di sicurezza, rilasciata da un'autorità indipendente equiparando, ad ogni effetto di legge, la firma digitale alla sottoscrizione autografa; infine la Francia, ove l'Assemblea Nazionale aveva approvato (il 24 febbraio 1998 e il successivo 23 marzo 1998), importanti modifiche della legge sulle telecomunicazioni (n. 90-1170 del 29 dicembre 1990) al fine di consentire l'uso di strumenti di crittografia finalizzati alla sottoscrizione digitale, mentre la Gran Bretagna aveva in corso, nello stesso periodo la revisione della legislazione vigente per favorire il libero svolgimento dell'attività di certificazione su autorizzazione dell'autorità pubblica e il riconoscimento legale delle firme digitali.

[11] F. DELFINI, *La recente direttiva sulle firme elettroniche: prime considerazioni*, in *I Contratti*, 2000, p. 424 ss.; F. SORRENTINO, *Firma digitale e firma elettronica: stato attuale e prospettive di riforma*, in *Il Diritto dell'informazione e dell'informatica*, 2000, p. 533 ss.; E. MORELATO, *Profili giuridici della firma elettronica nella direttiva comunitaria 1999/93/CE (raffrontata con il Modello di legge sulle firme elettroniche dell'UNCITRAL)*, in *Contratto e impresa*, 2001, p. 441 ss.; G. ARNÒ-D. LISTA, *La firma digitale nell'ordinamento italiano e comunitario*, in *Riv. dir. civ.*, 2000, II, p. 781 ss.

[12] Per firma digitale s'intende quel particolare metodo crittografico che consente di attribuire con certezza un documento, formato con strumenti informatici o trasmesso per via telematica, al suo autore grazie all'uso di due chiavi di cifratura (definite, rispettivamente, chiave « privata » e chiave « pubblica »). Il sistema è basato su funzioni matematiche « ad una via »: poiché ogni chiave può, indifferentemente, essere utilizzata per cifrare o decifrare, ma la chiave utilizzata per cifrare non può essere utilizzata per decifrare (e, cosa più importante, la conoscenza di una delle due chiavi non fornisce alcuna informazione per ricostruire l'altra chiave), una delle chiavi può essere resa pubblica ed utilizzata per la verifica della firma o per cifrare il contenuto del documento. Nel testo si danno, necessariamente, per noti al lettore i profili tecnologici della firma digitale e le principali modalità d'impiego delle tecniche crittografiche ideate, sul finire degli anni Settanta, da W. Diffie e M. Hellmann (nonché le funzioni matematiche necessarie per implementare questo schema in prodotti software di grande diffusione) successivamente scoperte dai matematici R. Rivest, A. Shamir e L. Adleman per garantire integrità, disponibilità e riservatezza del documento informatico. Per una descrizione approfondita, in termini storici e giuridici, della nascita e del funzionamento della firma digitale si rinvia a G. BUONOMO, *Il nuovo processo telematico*, Milano, 2009, pp. 82 e ss.; si veda anche A.M. GAMBINO, voce *Firma Digitale* (dir. civ.), in *Enc. giur. Treccani*, 1999, p. 3 ss. In generale, sull'uso della crittografia a chiavi asimmetriche per la firma dei documenti informatici, C. GIUSTOZZI, *Il nuovo ruolo della crittografia*, pp. 95 e ss., in C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti, spie e codici cifrati*, Milano, 1999. Sullo stesso tema, da ultimo, D. GIORIO, *Sicurezza informatica e crittografia* - Parte I-II, in *Lo stato civile italiano*,

La prima, e più importante, conseguenza giuridica di quest'approccio « tecnologicamente neutrale » ai prodotti di firma fu, pertanto, il riconoscimento, accanto ai sistemi di cifratura di stringhe rappresentative del testo, come la firma digitale, di combinazioni di dati usualmente utilizzate per accedere ai sistemi informatici, come l'uso dell'identificativo personale (*user ID*) associato ad una parola o sigla di riconoscimento (*password*).

Fece così ingresso nell'ordinamento comunitario la « firma elettronica », definita come una qualsiasi « associazione logica » in grado di connettere « dati in forma elettronica » ad altri « dati elettronici » al fine di essere utilizzati « come metodo di autenticazione[13] ».

La firma elettronica, nella vasta accezione introdotta dalla direttiva 1999/93/CE, serviva a identificare e a convalidare dati (come nel caso del PIN utilizzato per avere accesso ad un distributore automatico di banconote o ad un sistema di posta elettronica) con strumenti crittografici diversi dall'architettura a chiavi pubbliche.

La direttiva introdusse, inoltre, l'ulteriore categoria della « firma elettronica avanzata », definita dall'art. 2.2 come una firma elettronica « *a*) connessa in maniera unica al firmatario; *b*) idonea ad identificare il firmatario; *c*) creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; *d*) collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati ».

Questa definizione ben si adattava alle firme elettroniche basate su un'infrastruttura globale a chiave pubblica e sull'uso di strumenti crittografici (chiavi private e chiavi pubbliche) per la firma e la verifica dei documenti informatici, poiché apparve evidente che solo quelle firme che sono connesse in maniera unica al firmatario, e consentono l'identificazione dell'autore dello scritto, sono idonee a garantire le funzioni tipiche della firma di un documento (quella dichiarativa e quella indicativa, in primo luogo).

Dopo avere operato la fondamentale distinzione tra firme « elettroniche » e « firme elettroniche avanzate » (da intendere nel senso di « tecnologicamente progredite »), tuttavia, la direttiva precisò (con l'art. 5, comma 1) che solo le firme elettroniche avanzate, basate su un certificato qualificato e create mediante un dispositivo sicuro, possono essere equiparate, quanto ai « requisiti legali », alle firme autografe[14] (e conseguentemente valutate come idonee a costituire prova in giudizio)[15], imponendo agli Stati membri (art. 5, comma 2) l'adozione di ulteriori misure « ...affinché una

2009, pp. 785-788 e 864-867; C. CIANFRONE, *Crittografia e diritto: l'attuale stato dell'arte*, in *Ciberspazio e Diritto*, 2005, p. 445 ss.

[13] Ovviamente, quando si parla di « autenticazione » con riferimento ad un sistema informatico, si fa riferimento alla procedura di identificazione che consente l'accesso e l'uso del medesimo sistema. Opportunamente, l'art. 1, lett. *b*) del D.Lgs. n. 82/2005 definisce la « autenticazione informatica » come la « validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso ».

[14] Nel senso che queste firme « *...posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per i dati cartacei* » (art. 5.1., comma 1, lett. *a*).

[15] A questa disposizione si riferiscono quegli autori che ritengono la firma digitale come un terzo genere di firma elettronica (una firma caratterizzata dal particolare certificato che accompagna le chiavi, conforme alle disposizioni dell'allegato II della direttiva, definita « firma 5.1 »). Si veda, sul punto, M. CAMMARATA-E. MACCARONE,

firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che essa è in forma elettronica, o non basata su un certificato qualificato, o non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero non creata da un dispositivo per la creazione di una firma sicura » (principio di non discriminazione)[16].

In sostanza, nella direttiva del 1999 tutti i documenti sottoscritti con firma elettronica avanzata (non anche quelli muniti di una semplice firma elettronica) erano considerati idonei ad essere valutati in giudizio ai fini probatori, considerato che questi strumenti devono, comunque, consentire di identificare il firmatario, garantire l'integrità e l'immodificabilità involontaria del documento e un « controllo esclusivo » sul mezzo usato per firmare; ma solo i documenti associati ad un certificato rilasciato da un certificatore qualificato e firmati con uno strumento di firma « sicuro »[17] furono dichiarati astrattamente idonei ad essere equiparati ai documenti formati su carta e sottoscritti con firma autografa.

Pertanto, trascorso poco più di un anno dall'introduzione del testo unico sulla documentazione amministrativa[18] — D.P.R. 28 dicembre 2000, n. 445 — il 2 marzo 2002 entrò in vigore il D.Lgs. 23 gennaio 2002, n. 10 che, nell'introdurre le norme di recepimento della direttiva 99/93/CE sulle firme elettroniche, operò nuove e profonde modifiche al sistema (sostituendo, tra l'altro, il fondamentale articolo 10 del testo unico[19] sulla efficacia giuridica del documento informatico[20]).

La firma digitale sicura, Milano, 2003, p. 237.

[16] Rivestono fondamentale importanza, ai fini della definizione del quadro normativo sulle firme elettroniche, i quattro allegati della direttiva n. 93 del 1999 dedicate ai requisiti dei certificati qualificati (All. I), ai requisiti dei certificati qualificati (All. II), dei dispositivi sicuri per la generazione della firma (All. III) e alle « Raccomandazioni per la verifica della firma sicura » (All. IV). In particolare, i certificati qualificati devono includere: « *a*) l'indicazione che il certificato rilasciato è un certificato qualificato; *b*) l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione; *c*) il nome del firmatario del certificato o uno pseudonimo identificato come tale; *d*) l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto; *e*) i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario; *f*) un'indicazione dell'inizio e del termine del periodo di validità del certificato; *g*) il codice d'identificazione del certificato; *h*) la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato; *i*) i limiti d'uso del certificato, ove applicabili; e j) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili ».

[17] Si vedano in proposito le rettifiche della direttiva 1999/93/CE pubblicate in GU « L 13 » del 19 gennaio 2000) e in GU « L 119 » del 7 maggio 2002 (versione italiana).

[18] O. Troiano, *La firma elettronica qualificata tra armonizzazione sovranazionale e legislazioni nazionali*, in *Rivista critica del diritto privato*, 2004 fasc. 3, pp. 417 ss., sp. 431 osserva come l'art. 23.2 del D.P.R. 445/2000 avesse già previsto che « l'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo », ma che tale fattispecie non coincideva con quella comunitaria perché faceva riferimento alla sola firma digitale.

[19] L'art. 10 del D.P.R. n. 445/2000, come modificato dall'art. 6 del D.Lgs. n. 10/2002 disponeva che « Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa [...] piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto ».

[20] Su cui vedi C.M. Bianca, *La firma elettronica, si apre un nuovo capitolo*, in *Studium juris*, 2002, p. 1431 ss., sp. 1433

La nuova disposizione — che restò in vigore sino al 31 dicembre 2005 — fu aspramente criticata[21] perché impediva il disconoscimento della scrittura informatica distaccandosi dal modello dell'art. 2702 cod. civ. senza accogliere le norme della direttiva che imponevano una piena equiparazione tra i documenti informatici ed i documenti cartacei muniti di firma autografa.

Ulteriori modifiche furono successivamente introdotte dalla legge 16 gennaio 2003, n. 3, dal D.P.R. 7 aprile 2003, n. 137, e dal D.Lgs. 30 giugno 2003, n. 196, che andarono nuovamente ad incidere sulle norme del testo unico dedicate alla certificazione delle chiavi[22] e alle definizioni contenute nel primo articolo[23].

Fondamentale tappa di riordino è, pertanto, rappresentata dal codice dell'amministrazione digitale, emanato con D.Lgs. 7 marzo 2005, n. 82 (d'ora in avanti « CAD ») in attuazione della legge n. 229 del 2003[24], nell'ambito di quel processo di superfetazione normativa inaugurato da altre due « codificazioni » di quel periodo: il codice sulla protezione dei dati personali (emanato con D.Lgs. 30 giugno 2003, n. 196) e il codice delle comunicazioni elettroniche (D.Lgs. 1 agosto 2003, n. 259)[25].

ss.; F. DELFINI, *Il D.Lgs. n. 10/2002 di attuazione della direttiva 1999/93/CE in tema di firme elettroniche*, in *I Contratti*, 2002, p. 410 ss.

[21] Vedi diffusamente F. RICCI, *Scritture private e firme elettroniche*, Roma 2003, p. 163 ss.; O. TROIANO, *La firma elettronica qualificata tra armonizzazione sovranazionale e legislazioni nazionali*, cit., pp. 436-438; A. GRAZIOSI, *La nuova efficacia probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 2003, p. 53 ss., sp. 61-73.

[22] Questo confuso affastellarsi di norme correttive, integrative e modificative è visto da molti commentatori come un effetto, in gran parte prevedibile, della soppressione dell'AIPA e del venir meno delle funzioni di coordinamento che il D.Lgs. n. 39 del 1993 aveva affidato all'Autorità amministrativa indipendente. La mancanza di organicità del codice, che ha smembrato le norme del testo unico sulla documentazione amministrativa, è stata, in particolare, denunciata da G. DUNI, *L'e-government: dai decreti delegati del marzo 2005 ai futuri decreti entro il 9 marzo 2006*, in *Dir. Internet*, 2005, 2, 228 ss. e M. PIETRANGELO, *La società dell'informazione tra realtà e norma*, Milano, 2007, 89 e ss.

[23] Agli effetti deleteri di questa confusa iperproduzione legislativa vanno, tra l'altro, ricondotte le numerose imprecisioni contenute nelle disposizioni sul processo telematico (D.P.R. 13 febbraio 2001, n. 123), che si fondava in gran parte sull'uso della firma digitale nell'ambito del processo civile: basti pensare che, al momento della pubblicazione nella Gazzetta ufficiale (17 aprile 2001), il regolamento conteneva ancora numerosi riferimenti (artt. 1, 2, 3 ed 8) a disposizioni del D.P.R. n. 513 del 1997 che erano già abrogate.

[24] La legge di semplificazione per il 2001 muoveva dal dichiarato intento di raccogliere i numerosi e disorganici interventi normativi che si erano nel tempo stratificati sulla materia in un nuovo testo, più razionale e « semplificato ». La delega per il « riassetto in materia di società dell'informazione » era contenuta nell'art. 10 (per i fini che qui interessano) anche al fine di « graduare la rilevanza giuridica e l'efficacia probatoria dei diversi tipi di firma elettronica in relazione al tipo di utilizzo e al grado di sicurezza della firma » e « adeguare la normativa alle disposizioni comunitarie » e fu attuata con il D.Lgs. 28 febbraio 2005, n. 42, istitutivo del sistema pubblico connettività e della rete internazionale della pubblica amministrazione, e col D.Lgs. 7 marzo 2005, n. 82, recante il codice dell'amministrazione digitale. I decreti furono poi riuniti in un unico testo legislativo da un decreto integrativo e correttivo (D.Lgs. n. 159/2006) che apportò al testo originario sostanziali modificazioni. Sull'iter legislativo e sui dubbi di costituzionalità sollevati dall'adozione del decreto di modifica a così breve tempo dall'entrata in vigore del testo unico, si veda M. PIETRANGELO, in *La società dell'informazione tra realtà e norma*, Milano, Giuffrè, 2007, pagg. 63 e ss.

[25] Sull'ambizioso progetto di passaggio dai c.d. testi unici « misti », ai « codici »

Nel « codice », che negli intenti del legislatore avrebbe dovuto costituire lo strumento di attuazione della « rivoluzione digitale » della P.A., confluirono sia le norme sui documenti informatici che quelle sulle firme elettroniche, determinando i presupposti per il definitivo passaggio, nei rapporti tra amministrazioni pubbliche, cittadini ed imprese, dalla carta al documento informatico[26].

Peraltro, nel testo del decreto legislativo entrato in vigore il 1 gennaio 2006 la « firma avanzata » comunitaria lasciò (inspiegabilmente) il posto alla « firma elettronica qualificata », che riproduceva, tuttavia, quasi integralmente la definizione di « firma avanzata » contenuta nell'articolo 2 della direttiva comunitaria; mentre la « firma digitale » veniva definita come un particolare tipo di firma elettronica qualificata « basata su un sistema di chiavi crittografiche, una pubblica ed una privata, correlate tra loro ».

Pochi mesi dopo la sua entrata in vigore il codice subì nuove ed importanti modifiche per effetto del D.Lgs. 4 aprile 2006, n. 159, che aggiunse al corpo del codice un intero capo (l'ottavo) dedicato al Sistema pubblico di connettività (accorpando le norme precedentemente dettate dal D.Lgs. n. 42 del 2005)[27] e riscrisse i fondamentali articoli 20 e 21 del CAD.

Quanto all'efficacia probatoria del documento, il primo comma dell'art. 21 estese il libero apprezzamento del giudice alla integrità e immodificabilità, oltre che qualità e sicurezza, del documento informatico sottoscritto con firma elettronica; mentre il secondo comma stabilì che « L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria » introducendo nell'ordinamento una « presunzione di firma » destinata ad avere rilevanti conseguenze in tema di disconoscimento e di verificazione.

Le ultime modifiche sono storia recente: il D.Lgs. n. 235 del 2010 ha riscritto il comma 2 dell'art. 21, prevedendo un comma 2-*bis* che ha introdotto, sul piano sostanziale, la distinzione tra scritture forti e scritture deboli (laddove solo le prime, sottoscritte con firma elettronica qualificata o digitale, sono idonee a soddisfare la forma scritta *ad substantiam* contemplata dall'art. 1350, nn. 1-12, cod. civ.[28]); mentre, sul piano probatorio, il

in forma di decreti legislativi, teso a garantire un più incisivo intervento nelle singole materie, semplificandole al di là del « coordinamento formale » consentito per i testi unici, vedi N. LUPO, *Dai testi unici « misti » ai codici: un nuovo strumentario per le politiche di semplificazione. Commento alla legge n. 229 del 2003*, in *Studium iuris*, 2004, p. 157 ss.

[26] Vedi M. MORELLI, *La seconda fase della digitalizzazione nella pubblica amministrazione tra utopia e realtà*, in *Nuov. rass. leg., dott. e giur.*, 2005, p. 1123 ss.; N. LUGARESI, *Codice dell'amministrazione digitale e rapporti tra cittadino e Pubblica Amministrazione*, cit., p. 460. Per i primi rilievi critici, si veda M. SCIALDONE, *CAD: se la rivoluzione digitale resta sulla carta*, in *Il Nuovo Diritto*, 2007, V, pp. 275-277.

[27] Sul tema, C. D'ORTA, *Finalità, organizzazione e architettura del Sistema pubblico di connettività (SPC)*, in *Diritto dell'Internet*, 2005, p. 395 ss. Criticamente, A. NATALINI, *Il SPC eredita i problemi della RUPA*, in *Gior. dir. amm.*, 2005, p. 702 ss., il quale, ancor prima della sua introduzione, osservava come la nuova disciplina normativa fosse destinata a scontrarsi con le difficoltà insite nell'introduzione di forme di concertazione istituzionale e ne lamentava la tendenza a concentrare l'attenzione, in continuità con la RUPA, sulla diffusione delle tecnologie dell'informazione e della comunicazione negli uffici amministrativi, lasciando in secondo piano i problemi connessi al loro proficuo utilizzo.

[28] F. RICCI, *Firma Digitale*, in *Diritto Civile*, a cura di S. Martuccelli-V. Pescatore, Milano 2011, p. 783 ss., sp. 786.

nuovo comma 2 ha attribuito l'efficacia prevista dall'articolo 2702 cod. civ. non più ai soli documenti sottoscritti con firma digitale o con un altro tipo di firma elettronica qualificata, ma ad ogni documento informatico « sottoscritto con firma elettronica avanzata, qualificata o digitale, [...] che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento ». Fino ad arrivare, come detto in premessa, alla recentissima legge n. 221 del 2012[29], che ha (definitivamente?) dettagliato il sistema intervenendo, nuovamente, sul piano dell'efficacia tanto sostanziale quanto probatoria.

3. Documento e scrittura informatica.

Una ricognizione del valore probatorio della scrittura privata informatica, nell'ambito del quadro normativo vigente, non può prescindere dalla considerazione del documento informatico come documento *scritto* su un supporto informatico.

Contrariamente a quanto immaginato da alcuni commentatori[30], l'introduzione del documento informatico non ha svincolato l'essenziale funzione di conservazione del contenuto rappresentativo dall'esistenza di un supporto materiale; anche se è evidente che il legislatore, nel ricondurre (con la definizione offerta dal codice dell'amministrazione digitale, e prima ancora dal testo unico 445/2000) il documento informatico a « rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti » (art. 1 lett. p, CAD), coglie soltanto una specificità della rappresentazione documentale, senza assorbire in essa una completa definizione del documento informatico[31].

« Rappresentazione informatica » significa, in primo luogo, « rappresentazione su un supporto informatico », posto che la definizione introdotta dal CAD richiama, con pochi aggiustamenti, la tradizionale definizione

[29] Che ha convertito con modificazioni il decreto legge 18 ottobre 2012, n. 179 e ha disposto con l'art. 9, comma 1, let. 0*a*) la modifica dell'art. 21, comma 2; e con l'art. 9, comma 1, let. 0*b*) la modifica dell'art. 21, comma 2-*bis*.

[30] P. Tonalini, *La sottoscrizione elettronica dei documenti*, in *Studium juris*, 1997, p. 442; G. Rognetta, *La firma digitale e il documento informatico*, Napoli 1999, p. 165 e ss.; G. Ciacci, *La firma digitale*, cit., p. 77; A. Masucci, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 2004, p. 749 ss., sp. 755 ss. Secondo la tesi (che qui si contesta) di M. Cammarata-E. Maccarone, *La firma digitale sicura*, cit., p. 55 « ...in nessun punto della normativa sul documento informatico il supporto è determinante per la natura del documento stesso » poiché « Esso esiste indipendentemente dal supporto, è una realtà immateriale, cioè l'esatto opposto della *res signata* della dottrina tradizionale ». Al contrario, la tesi qui esposta individua nel supporto informatico e nel codice binario i caratteri distintivi del documento informatico, sicché esso dev'essere considerato, pur sempre, un documento scritto, ancorché su un supporto diverso dalla carta.

[31] G. Finocchiaro, *La firma digitale (artt. 2699-2720). Supplemento D.P.R. 10 novembre 1997, n. 513*, in *Commentario del codice civile Scialoja-Branca* a cura di F. Galgano, Bologna-Roma 2000, p. 30 e ss.; M. Miccoli, *sub art. 1*, in *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, cit., p. 646. Per G. Navone, *Il documento informatico in confronto alle altre res documentales*, cit., p. 239, la dizione legislativa testimonia « la maturata consapevolezza di non poter considerare il documento informatico semplicemente alla stregua di un nuovo oggetto materiale, contraddistinto esclusivamente per la peculiare natura fisica del supporto contenente ».

di documento (quale « rappresentazione di atti o fatti giuridicamente rilevanti »[32]) e, con essa, la teoria « rappresentativa » accolta nel codice civile (secondo cui il documento è destinato a raccogliere, a futura memoria, su un supporto di qualsiasi tipo, la rappresentazione di fatti o atti giuridicamente rilevanti[33]). Dunque, un contratto, scritto su tavolette cerate, su pietra o pergamena, resta pur sempre un atto in forma scritta, quale che sia la natura del corpo recettore a cui è affidato il compito di trattenere le informazioni nel tempo[34].

Così, seguendo l'evoluzione delle conoscenze scientifiche e tecnologiche, l'avvento dell'informatica ha condotto a sostituire il tradizionale supporto cartaceo con diversi tipi di supporti alternativi costituiti da dischi magnetici contenuti in custodie di materiale plastico flessibile (floppy-disk), da dischi a lettura ottica (CD-ROM - DVD-ROM) e, da ultimo, dalle memorie « a stato solido ». Ma, in ogni caso, per garantire e preservare nel futuro la testimonianza di un fatto (ad esempio, una dichiarazione negoziale) o per formare una dichiarazione (ad esempio, un provvedimento amministrativo) il documento è sempre costituito da una informazione diretta all'altrui conoscenza e veicolata da un elemento fisico (il supporto su cui è registrata l'informazione).

Tuttavia, pur nella perdurante consapevolezza che non esiste un documento senza rappresentazione[35], e che tale rappresentazione non può prescindere da un supporto di registrazione delle informazioni destinate a conservarsi nel tempo, occorre chiarire come la specificità del documento informatico non può esaurirsi nelle peculiarità del contenente[36].

[32] Si veda, *ex multis* F. CARNELUTTI, *Documento e negozio giuridico*, in *Riv. dir. proc.*, 1926, I, 181 ss.; ID., voce *Documento (teoria moderna)*, in *NN. D.I.*, VI, Torino, 1960, 86 ss.; E. BETTI, *Diritto processuale civile italiano*, Roma, 1936, p. 356.

[33] Come noto, il codice civile italiano non contiene una definizione di documento pur adoperando tale termine in diverse disposizioni (ad es., artt. 736, 1262, 1477, 2235, 2961 cod. civ.) ed il capo dedicato alla prova documentale si riferisce non soltanto al documento scritto ma ad una serie di altri strumenti di fissazione o riproduzione di fatti, comunque rientranti nella disciplina legislativa. Osserva, pertanto, L. CARRARO, *Il diritto sul documento*, Padova 1941, p. 7-8, che « vi possono essere cose rappresentative che non sono documenti » e, pertanto, il documento sarebbe soltanto la « cosa rappresentativa di un fatto giuridicamente rilevante » ovvero la cosa rappresentante un oggetto in grado di avere un'influenza nel mondo giuridico.

[34] Un'approfondita discussione sulla natura giuridica e funzione del documento, così come sulla funzione della sottoscrizione e, in generale, della scrittura come mezzo di prova della volontà negoziale eccede, evidentemente, i limiti di questa trattazione. Per una ricognizione essenziale della tradizionale dottrina sul documento si rimanda a L. CARRARO, *Il diritto sul documento*, cit.; F. CARNELUTTI, *Documento (Teoria moderna)*, cit., p. 85; P. GUIDI, *Teoria Giuridica del documento*, Milano, 1950; A. MORELLO, voce *Sottoscrizione*, in *NNDI*, XVII, Torino 1978, 1003 ss.; C. ANGELICI, voce *Documentazione e documento*, *Diritto civile*, in *Enc. giur.*, Roma, 1989., p. 3 ss.; S. PATTI, voce « *Documento* », in *Digesto delle discipline privatistiche*, *sez. civ.*, VII, p. 1 ss.

[35] Contrariamente, rigetta l'idea del documento in quanto cosa rappresentativa, C. ANGELICI, voce *Documentazione e documento*, op. cit., p. 1, negando, in particolare, che il documento sia di per sé in grado di rappresentare oggettivamente un fatto, poiché il significato del documento dipende da chi interpreta o intende i segni in esso fissati.

[36] Peraltro, è opportuno rammentare come la natura della materia che accoglie i segni non abbia mai condizionato il dibattito sulla nozione di documento, essendo ampiamente condivisa l'opinione che opta per la sostanziale irrilevanza della materia nella quale il documento, di volta in volta, si sostanzia. Si veda A. MALINVERNI, *Teoria del falso documentale*, Milano 1958; G. LASERRA, *La Scrittura privata*, Milano 1959,

In questo senso, non convincono le tesi che individuano tale specificità nell'intrinseca delebilità del supporto[37], vale a dire l'incapacità strutturale delle memorie informatiche di conservare traccia, in qualche modo riconoscibile all'esterno, delle modifiche e/o alterazioni subite dai dati in esse archiviati[38], poiché un conto è la verifica dell'integrità del documento (destinata a condizionarne l'efficacia probatoria) ed un conto è, invece, la riconoscibilità del documento in quanto registrazione di atti, fatti o dati giuridicamente rilevanti su un supporto informatico, quale che sia[39].

Parimenti, non sembra cogliere nel segno la tesi che vede nell'indiretta visibilità del documento informatico — in quanto non intellegibile con organi di senso ma solo tramite la mediazione ed elaborazione di macchine traduttrici (*computer* e dispositivi informatici) — il tratto che lo distingue dal documento in genere[40], poiché si tratta di un requisito obiettivo[41] che non è esclusivo dei documenti informatici[42].

In funzione della natura del fatto rappresentato e della relativa rappresentazione, anche per i documenti informatici è possibile distinguere tra le riproduzioni informatiche, che raffigurano direttamente un fatto attraverso il mezzo figurativo (e sono riconducibili all'ambito delle riproduzioni *ex machina* dell'art. 2712 cod. civ.) e le scritture informatiche che, invece, risultano formate attraverso il ricorso al mezzo verbale ed ai segni propri del linguaggio scritto (si pensi alla contrattazione telematica ed al c.d. fenomeno dell'*e-commerce*[43]).

p. 164 e ss.; F. CARNELUTTI, *Documento (Teoria moderna)*, cit., p. 86; S. PATTI, *Prova documentale (artt. 2699-2720)*, in *Commentario del Codice Civile Scialoja-Branca*, a cura di F. GALGANO, Bologna-Roma, 1996, p. 8 ss.; con specifico riferimento al documento informatico, vedi R. CLARIZIA, *Informatica e conclusione del contratto*, Milano 1985, p. 100 ss.; R. BORRUSO, *Computer e diritto. Problemi giuridici dell'informatica*, tomo II, Milano 1988, p. 218 ss.

[37] Indelebilità espressamente riconosciuta da Cass. civ., sez. III, 29 gennaio 1999, n. 795, in *Vita notarile* 1999, I, p. 369; Cass. pen., sez. III, 1 febbraio 1996, n. 3110, in *Riv. pen.*, 1996, p. 583.

[38] Vedi F. PARISI, *Il contratto concluso mediante computer*, Padova 1987, p. 70 e ss.; M. ORLANDI, *La paternità delle scritture - sottoscrizione e forme equivalenti*, Milano 1997, p. 97 e ss.

[39] Diversamente, occorrerebbe escludere dalla categoria dei documenti informatici quelli che non sono muniti di firma elettronica (o sono muniti di firma elettronica non avanzata), contrariamente a quanto è dato evincere dal chiaro dispone l'art. 21, comma 1, del CAD che semplicemente degrada l'efficacia probatoria di quei documenti informatici, come meglio vedremo più avanti, rendendoli liberamente apprezzabili dal giudice, analogamente alle riproduzioni meccaniche *ex* art. 2712 cod. civ., in considerazione delle loro « caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità ».

[40] E. GIANNANTONIO, *Il valore giuridico del documento elettronico*, in *La forma degli atti nel diritto privato. Studi in onore di Michele Giorgianni*, Napoli 1988, p. 383. Più di recente, A. GRAZIOSI, *Parola detta, parola scritta e parola telematica, questioni in tema di prova e provenienza.* in AA.VV., *Scrittura e diritto*, Milano 2000, sp. 168: « la differenza rispetto alla parola scritta sta semplicemente nel fatto che la rappresentazione della parola telematica, agli occhi del lettore destinatario, non avviene immediatamente, ma necessita sempre e comunque dell'intermediazione di una macchina, che è appunto l'elaboratore elettronico ».

[41] Si veda A. GRAZIOSI, *Documento informatico (diritto processuale civile)*, in *Enc. Dir. Annali*, II, t. 2, Milano 2008, p. 495 parla di « rappresentatività indiretta », quale caratteristica peculiare del documento informatico.

[42] È evidente, infatti, come anche documenti fonografici e/o cinematografici possono essere uditi o visti solo attraverso la mediazione di appositi impianti audio, giradischi, proiettore di immagini, ecc. Sul tema, F. VIGLIONE, *L'imputazione dei documenti tra crisi della sottoscrizione e innovazioni tecnologiche*, in *Riv. dir. civ.*, 2003, p. 243 e ss., spec. 246.

[43] In argomento, *ex multis*, C.M. BIAN-

A prescindere dalla natura di riproduzione o di scrittura, oltre che dal carattere dichiarativo o narrativo di quest'ultima, costituisce condizione necessaria e sufficiente, ai fini della concessione della qualità di documento, l'attitudine a soddisfare l'essenziale funzione di perpetuazione di un determinato contenuto rappresentativo nel tempo attraverso un mezzo atto ad imprimere un segno su un supporto materiale[44]; ed a noi pare che il documento informatico sia contraddistinto proprio dalla qualità dei segni che reca impressi[45]: i *bit* resi per il tramite del linguaggio binario[46], che offrono la rappresentazione dell'atto o del fatto giuridicamente rilevante[47].

Il supporto che incorpora la concatenazione dei segni è imprescindibile, poiché senza di esso la sequenza diventerebbe evanescente[48], ma è il carattere del segno, che nel caso di specie prende forma attraverso la sequela d'impulsi elettrici binari, a connotare il documento informatico come insieme di dati espressi in forma elettronica ed utilizzati come metodo di rappresentazione informatica.

Peraltro, rapportandoci alla scrittura (informatica) a carattere dichiarativo[49] ed al ruolo di elemento costitutivo che in essa svolge la sottoscrizione, è possibile osservare come la stessa firma elettronica, tanto semplice quanto avanzata, sia sempre definita come « insieme dei dati in forma elettronica », indicazione che esplicita la duplice esigenza che la firma possa aderire al documento da sottoscrivere e che, per farlo, debba essere omogenea agli altri segni che quel documento compongono e caratterizzano[50].

CA, *I contratti digitali*, in *Studium juris*, 1998, p. 1035 ss.; G. DE NOVA, *Un contratto di consumo via Internet*, in *Contratti*, 1999, p. 113 ss.; R. CLARIZIA, *Il contratto informatico*, in MAZZAMUTO (a cura di), *Il contratto e le tutele. Prospettive di diritto europeo*, Torino, 2002, p, 694 ss.; F. AZZARRI, *La conclusione dei contratti telematici nel diritto privato europeo*, in *Contratti*, 2010, p. 301 ss.

[44] G. NAVONE, *Il documento informatico in confronto alle altre res documentales*, cit., p. 259, ben coglie l'esigenza di spiegare « l'apparente paradosso di un documento che, pur non identificandosi nella singola *res signata*, abbisogna della forma palpabile e solida di qualche oggetto ». L'Autore, peraltro accoglie l'idea dell'immaterialità del supporto, qui non condivisa.

[45] Per N. IRTI, *Forma del contratto e prova*, in *Le prove nel diritto civile e tributario*, a cura di C. Glendi, S. Patti, E. Picozza, Torino 1986, p. 33: « i segni grafici s'incorporano sempre, per fisica necessità, in una cosa rappresentativa ».

[46] *Bit*, come noto, è l'acronimo di *binary digit*, elemento « atomico » dell'informazione digitale, caratterizzato dalla presenza (1) o dall'assenza (0) di un impulso elettrico. Cosa diversa, pur rimanendo nel campo dell'elettronica, è, invece, il segnale analogico, in grado di variare in relazione alla grandezza fisica che misura, potendo esprimere un insieme infinito di valori in un campo continuo.

[47] Analogamente, F. RICCI, *Firma Digitale*, in *op. cit.*, p. 784, che osserva: « In questo modo tutte le informazioni documentate non solo esprimono concetti, ma corrispondono sempre a grandezze numeriche del sistema a base due (c.d. sistema binario) e possono pertanto essere misurate e messe in relazione tra loro ».

[48] Cfr., F. RIZZO, *Il documento informatico. Paternità e falsità*, Napoli, 2005, p. 269.

[49] Sulla distinzione tra documento e dichiarazione, F. CARNELUTTI, *La prova civile*, Roma, 1947, 134 ss., ha ben chiarito come lo scrivere sia forma di una dichiarazione, mentre lo scritto è il documento della dichiarazione: « L'evitar la confusione tra i due termini è una vera necessità logica, poiché la dichiarazione (negozio) è un atto, il documento è un oggetto il requisito formale della dichiarazione non è punto il documento, ma la formazione del documento; in altri termini ciò che importa per la forma è lo scrivere (atto), ciò che importa per la prova è lo scritto (oggetto) ».

[50] Cfr. F. RICCI, *Firma Digitale*, cit., p. 785, secondo cui « ogni firma deve essere espressa nella medesima forma elettronica dei dati ai quali si riferisce per poter essere documentata insieme a loro ».

4. Le diverse tipologie di firme elettroniche.

Nel testo attualmente in vigore, il codice dell'amministrazione digitale individua quattro distinte categorie di firme: la *firma elettronica*, che è definita come « l'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*, definita come « l'insieme di dati in forma elettronica allegati oppure connessi 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*, consistente in « un particolare tipo di firma elettronica avanzata [...] basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 lett. *r*) e, infine, la *firma digitale*, definita come « un particolare tipo di firma elettronica *avanzata* 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 di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici » (art. 1 lett. *s*).

Si tratta, dunque, di una serie di definizioni correlate tra loro attraverso un complesso sistema di riferimenti che, una volta definite le due categorie generali, rappresentate dalla firma elettronica (« dati associati ad altri dati ») e dalla firma avanzata (« dati associati ad un documento »), riconduce sia la firma « qualificata » sia la firma « digitale » alla firma « avanzata » (di cui possiedono entrambe i requisiti della « riconducibilità » al titolare, del « controllo esclusivo » sul mezzo di firma e dalla « immodificabilità » dei dati) per poi distinguerle in ragione del « certificato qualificato » — la firma qualificata — o del « sistema di chiavi crittografiche » — la firma digitale— su cui esse sono « basate »[51].

Il PIN digitato sulla tastiera del *cash dispenser* costituisce un esempio di firma elettronica: chi deve prelevare danaro contante si fa identificare dal sistema informatico come titolare del conto corrente bancario facendo ri-

[51] Con le modifiche all'art. 1 introdotte dall'art. 1, comma 1, lett. *g*) del D.Lgs. n. 235 del 2010, la firma digitale viene ora definita come un particolare tipo di firma « avanzata », a differenza della precedente definizione (rimasta in vigore dal 14 maggio 2006 al 24 gennaio 2011) che faceva riferimento alla firma digitale come ad un « particolare tipo di firma elettronica *qualificata* ». In questo modo, la firma digitale ha perso il riferimento al « dispositivo sicuro », proprio della firma qualificata, anche se occorre considerare che la direttiva comunitaria conosce solo due tipi di firma (quella « elettronica » e quella « avanzata ») e che anche la firma avanzata si caratterizza per l'uso di « mezzi sui quali il firmatario può mantenere un controllo esclusivo » (che, nel caso della firma digitale, dovrebbero coincidere con lo « strumento sicuro di firma » dell'allegato III della direttiva. Si tratta, come non ha mancato di rilevare la più attenta dottrina, di un evidente errore del legislatore che rischia di rendere la firma digitale « [...] meno sicura della firma elettronica qualificata, non essendo la prima necessariamente basata su un dispositivo sicuro ». Sul punto, G. Finocchiaro, *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, in *Contratto e impresa*, 2011, p. 499.

corso ad una firma elettronica comune costituita da dati elettronici (il PIN) associati ad altri dati[52] (il numero di carta), che il sistema è programmato per collegare al suo titolare prima di erogare il servizio. Allo stesso modo, chi deve spedire un messaggio di posta elettronica si fa identificare dal fornitore del servizio inserendo il proprio nome-utente e la parola di accesso[53].

La firma elettronica, pertanto, è sempre usata in funzione indicativa (o identificativa, che dir si voglia) e non ha, al contrario della firma avanzata, anche funzione dichiarativa[54].

Un esempio di firma avanzata è offerto, invece, dalla *firma grafometrica*, che consiste nella firma autografa apposta con un pennino su una tavoletta elettronica (*tablet*) che ne rileva istantaneamente non solo il tratto grafico ma anche velocità, precisione, angolo di inclinazione, accelerazione e il numero di volte in cui la penna viene sollevata dal piano di scrittura. Un apposito programma applicativo provvede, istantaneamente, ad analizzare la firma confrontandola con le scritture campionate in precedenza: i dati biometrici, nelle applicazioni più avanzate, vengono quindi

[52] Da questo punto di vista non è da condividere l'idea secondo cui « i vari esempi di firma elettronica 'semplice' individuano codici identificativi associati ad un documento informatico »; cfr. F. ROTA, *Il documento informatico*, in M. TARUFFO, *La prova nel processo civile*, *Trattato di diritto civile e commerciale Cicu-Messineo*, Milano, 2012, p. 723 ss., sp. 742.

[53] La giurisprudenza di merito ha più volte affermato che un messaggio di posta elettronica, non firmato, costituirebbe un documento informatico sottoscritto con firma elettronica c.d. semplice, in quanto il mittente, per poter creare ed inviare la e-mail, deve eseguire un'operazione di validazione inserendo il proprio identificativo individuale (*username*) ed il proprio codice di accesso (*password*); si veda Trib. Prato, 15 aprile 2011, in *Foro it.*, 2011, I, c. 3198 e *Corr. merito*, 2011, p. 802, con nota di C. SGOBBO, *Il valore probatorio della e-mail*, p. 803 ss.; si veda anche, nella vigenza dettato normativo del D.P.R. 445/2000, n. 445, GdP Pesaro 2 novembre 2004, in *Giur. it.*, I, 2005, c. 1024. Su tale base, non di rado si è giunti a concludere che la semplice e-mail costituisce prova scritta ai sensi degli artt. 633, n. 1 e 634 cod. proc. civ. per l'emanazione di un decreto ingiuntivo; si vedano Trib. Verona 26 novembre 2005, in *Giur. Merito*, 2005, p. 2129; Trib. Mondovì 7 giugno 2004, in *Nuova giur. civ. comm.*, 2005, I, p. 936 ss., con nota di M. LUPANO, *Natura dell'*e-mail, *sua efficacia probatoria nella normativa vigente e nel D.Lgs. 7 marzo 2005*, n. 82; Trib. Cuneo 15 dicembre 2003, in *Giur. merito*, 2005, I, p. 560, con nota di M. PANI, *Il valore di prova scritta di una e-mail: la giustizia inizia a porsi al passo coi tempi* e in *Dir. Internet*, 2005, p. 33 ss., con nota di G. ROGNETTA, *Decreti ingiuntivi basati su e-mail: la configurabilità della firma elettronica ai fini della prova scritta*. Va notato, tuttavia, che i codici di identificazione, per essere utilizzati come firma del documento, vanno inviati al destinatario del messaggio e non al fornitore del servizio di posta. In questo caso, dunque, il messaggio non è firmato e la firma elettronica costituita dalla combinazione *username-password* ha il solo scopo di far identificare il mittente dal fornitore del servizio di posta elettronica. Ne consegue che, come confermato dal parere del Consiglio di Stato del 30 Gennaio 2006 sulla bozza del futuro D.Lgs. n. 159/2006, il documento inviato via e-mail non potrebbe mai dirsi, per ciò solo, sottoscritto. Analogamente, M.G. JORI, *L'efficacia probatoria dell'e-*mail, in *Giur. it.*, 2005, p. 1028 ss.; M. FARINA, *Riflessioni sul valore legale* delle e-mail *a seguito della pronuncia di alcuni decreti ingiuntivi basati esclusivamente sulla produzione di una* e-mail, in *Rass. dir. civ.*, 2005, p. 615 ss.

[54] Infatti, tale metodo di identificazione informatica, basato sulla conoscenza di un dato « segreto », non consente l'identificazione certa del soggetto agente, poiché il dato è conosciuto o conoscibile anche da persone diverse dal firmatario, come ad esempio dal gestore del sistema con cui l'utente interagisce. Si veda R. BORRUSO, *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (D.Lgs. 23 gennaio 2002, n. 10, D.P.R. 7 aprile 2003, n. 137 e L. 29 luglio 2003, n. 229)*, in *Gius. civ.*, 2004, II, p. 143 ss., sp. 164.

« incorporati » nella firma e associati, con essa, al documento (nel senso che i dati rilevati durante la firma divengono, sostanzialmente, la chiave privata con cui viene apposta la firma digitale sul documento).

È evidente che in questo genere di applicazioni (che sono sempre più diffuse soprattutto in ambito bancario) i dati raccolti durante la firma sono creati con lo stesso gesto con cui si appone una firma autografa su un foglio di carta (sicché è la mano del firmatario, in ultima analisi, il mezzo che garantisce il « controllo esclusivo » del titolare) e consentono di rilevare successive modifiche attraverso la stessa tecnologia dei codici cifranti di cui si avvale la firma digitale.

Più difficile è trovare un esempio di firma « qualificata », che si caratterizza, come detto, per il certificato qualificato[55] e per l'uso del dispositivo sicuro.

Secondo la maggioranza degli studiosi, solo la tecnologia basata sulle chiavi asimmetriche di cifratura consentirebbe di incorporare la firma nel documento in modo indissolubile, garantendo l'integrità e l'autenticità dello scritto[56]; sicché non esisterebbe, allo stato delle attuali conoscenze scientifiche e tecnologiche, una firma « qualificata » distinguibile dalla firma digitale.

Tuttavia, qualche distinzione potrebbe farsi anche in questo caso, traendo spunto dalle numerose applicazioni in uso per la gestione a distanza dei rapporti bancari.

Chi deve comunicare il numero della propria carta di credito alla banca attraverso l'internet utilizza, di norma, connessioni « sicure » realizzate con l'uso di chiavi di cifratura « usa e getta » generate al momento della connessione; cosicché, una volta cifrati i dati da trasmettere con la chiave pubblica, solo il possessore della chiave privata (la banca) è in grado di effettuare l'operazione inversa, decifrando il messaggio[57].

Per aumentare la sicurezza della trasmissione, alcune banche consegnano ai loro clienti anche un apparecchio generatore di un codice numerico pseudocasuale ad intervalli regolari (di norma, variabile ogni dieci se-

[55] Nell'architettura a chiavi crittografiche pubbliche, il certificatore è tenuto ad identificare « con certezza » (art. 32 CAD) colui che richiede il rilascio del certificato con cui vengono accompagnati i documenti sottoscritti con firma digitale. I requisiti di questo attestato elettronico sono contenuti nell'art. 28 del CAD e nell'allegato I della direttiva comunitaria n. 93 del 1999. Solo le firme elettroniche avanzate, basate su un certificato qualificato e create mediante un dispositivo sicuro, sono equiparate, quanto ai « requisiti legali » alle firme autografe e sono ammesse come prova in giudizio, secondo le disposizioni dell'art. 5, comma 1, della stessa direttiva. Sull'art. 30 CAD ed il delicato tema della responsabilità del certificatore, si veda I. LUCATI, *Certificatori: responsabilità e sanzioni*, in *La resp. civ.*, 2011, p. 157 ss.

[56] G. DUNI, voce: *Amministrazione digitale*, cit., p. 13. Anche secondo A. GRAZIOSI, voce: *Documento informatico (dir. proc. civ.)*, in *Enc. dir. - Annali vol. 2*, Milano, 2007, p. 500, il confronto tra la definizione di firma avanzata e quella di firma qualificata evidenzierebbe « che si tratta della stessa cosa ». Dello stesso parere sembra A. VILLECCO, *Il processo civile telematico*, Torino, 2011, p. 25, in nota. Secondo G. FINOCCHIARO, *Ancora novità legislative*, cit., p. 499, « La "firma elettronica qualificata" è [...] un'espressione sintetica che si riferisce alla "firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo per la creazione di una firma sicura", cui la direttiva collega determinati effetti giuridici ».

[57] La firma qualificata, dunque, è una specie appartenente al genere delle firme avanzate, poiché si tratta, pur sempre, di firme elettroniche basate su una infrastruttura a chiavi pubbliche (PKI).

condi) denominato *token* (gettone) e sincronizzato con un server di autenticazione che genera la stessa sequenza di numeri pseudocasuali sotto il controllo della banca. Poiché la password temporanea per l'autenticazione varia col passare del tempo, solo chi possiede il *token* è in grado di generare, nel preciso istante in cui viene richiesta la password di autenticazione, lo stesso numero pseudocasuale generato dal server; e solo il titolare del conto corrente conosce la password di partenza con cui il numero va combinato[58].

In questo schema di sicurezza informatica, dunque, il canale sicuro, su cui il codice viene trasmesso dal titolare alla banca, viene creato attraverso la cifratura del messaggio con la chiave pubblica generata dal ricevente (la banca): a destinazione, pertanto, il messaggio viene decifrato con l'altro elemento della coppia (la chiave privata, rimasta nel possesso della banca che l'ha generata) e poi viene eliminata.

Si tratta, pur sempre, di una architettura PKI (a chiavi asimmetriche di cifratura); ma il certificato, emesso da un certificatore qualificato, accompagna una chiave (pubblica) utilizzata solo per cifrare temporaneamente (rendendolo non intelligibile ad alcuno, al di fuori del destinatario) il messaggio contenente il codice temporaneo e non anche per « rendere manifesta e verificare la provenienza e l'integrità di un documento informatico » secondo la definizione di firma digitale contenuta nell'art. 1, lett. *s*) del CAD.

La « firma qualificata » (se di questo si tratta) è dunque una specie di firma avanzata; ma essa non coincide, esattamente, con una firma digitale che si appone al documento utilizzando l'altro elemento della coppia (la chiave privata)[59].

In altri termini, la tecnologia utilizzata (l'algoritmo RSA) è la medesima utilizzata per la firma digitale, ma è evidente come, con questa operazione, il mittente non intenda « firmare » un documento ma, semplicemente, farsi identificare dal sistema per accedere ai relativi servizi, utilizzando uno strumento « sicuro » sul quale egli mantiene un controllo esclusivo.

Numerosi sono, infine, gli esempi di firma digitale, che consiste nell'applicazione, sul documento formato con strumenti informatici o trasmesso per via telematica, di una sequenza di caratteri alfanumerici che sono il prodotto di un'operazione di cifratura eseguita con un sistema crittografico a chiavi asimmetriche (ove la chiave usata per cifrare non può decifrare, anche se l'operazione può essere iniziata con uno qualsiasi degli elementi della coppia)[60].

[58] In pratica, poiché la password temporanea scade dopo pochi secondi, per forzare il sistema occorrerebbe conoscere il codice temporaneo ed usarlo, al posto del titolare, prima della scadenza.

[59] Ciò che distingue la firma digitale (« 5.1 ») da una firma avanzata (che si chiama così perché è « tecnologicamente avanzata » rispetto ad una comune firma elettronica) non è un'essenziale diversità tecnologica ma soltanto la rispondenza dell'attestato emesso dal certificatore, e del meccanismo utilizzato per l'operazione di cifratura, a particolari requisiti di forma e contenuto più rigorosi.

[60] Su cui, in dottrina, *ex multis*, F. Ricci, *Firma Digitale*, cit., p. 787; Id., *Scritture private e firme elettroniche*, cit., p. 108 ss.; R. Borruso-G. Ciacci, *Diritto civile e informatica*, Napoli, 2004 p. 408 ss.; M. Cammarata-E. Maccarone, *La firma digitale sicura*, cit., p. 28 ss.; R. Zagami, *Firma digitale e sicurezza giuridica*, cit., p. 33 ss.; G. Finocchiaro, *La firma digitale*, cit., pp. 1-28 e p. 41 ss.; A.M. Gambino, *Firma digitale (dir. civ.)*, in *Enc. giur.*, XIV, Roma, 1999.

L'operazione di firma consiste nell'estrarre, dal testo che compone il documento, un campione rappresentativo (denominato « valore di *hash* » o « *message digest* ») e nel cifrare, con una delle chiavi (« chiave privata ») la stringa di caratteri così ottenuta.

La « firma » digitale è, dunque, il prodotto di questa operazione crittografica, consistente in una sequenza fissa di caratteri alfanumerici (poiché fisso è il numero dei caratteri della sequenza rappresentativa cifrata) posta in calce al testo (o in un file ad esso associato inscindibilmente)[61].

Il codice dell'amministrazione digitale esige (art. 1 lett. s) e art. 21) che il sistema di chiavi crittografiche sia basato su un certificato emesso da un certificatore qualificato e che la firma sia (attraverso il richiamo alla definizione di firma avanzata) « creata con mezzi sui quali il firmatario può conservare un controllo esclusivo ». Tuttavia, ciò non toglie che la tecnologia basata sulle chiavi asimmetriche di cifratura possa essere utilizzata anche per firmare un documento informatico senza far ricorso, necessariamente, alla certificazione delle chiavi[62].

In conclusione, posto che l'uso di un « certificato » elettronico, per collegare all'identità del titolare i dati utilizzati per verificare le firme elettroniche, è tipico dell'architettura a chiavi pubbliche (PKI), e che anche la firma grafometrica deve utilizzare la tecnologia RSA per associare inscindibilmente i dati biometrici del firmatario al documento, le firme avanzate possono distinguersi tra firme che non fanno uso di certificati (e, tra queste, la più importante applicazione è costituita dalla firma grafometrica) e firme che si avvalgono, invece, dei soggetti certificatori (*in primis*, la firma digitale).

Per completare il quadro, va ricordato che le norme del codice dell'amministrazione digitale vanno integrate con le regole tecniche (D.P.C.M. 22 febbraio 2013) che, con riferimento (praticamente esclusivo) alla firma digitale, dispongono che *a*) una coppia di chiavi per la creazione e la verifica della firma può essere attribuita ad un solo titolare; *b*) le chiavi di sottoscrizione, destinate alla generazione e verifica delle firme sui documenti, possono essere utilizzate solo per firmare, così come le chiavi di certificazione e quelle di marcatura temporale non possono essere utilizzate per scopi diversi da quelli per cui sono state generate (art. 5); la generazione della firma deve avvenire all'interno di un dispositivo sicuro di firma, così che non sia possibile l'intercettazione della chiave privata utilizzata; il dispositivo sicuro di firma deve essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma (art. 11)[63].

[61] In altri termini: dato un testo « A » ed estratto da questo il digest « B », si ottiene una firma digitale cifrando, con una chiave privata, il testo « B ». La firma è, quindi, il prodotto della cifratura di una sequenza di caratteri rappresentativa del testo e di lunghezza fissa (le dimensioni della firma, cioè, non dipendono dalla lunghezza del testo, pur essendo la firma un sistema crittografico applicato al testo).

[62] Alcuni programmi informatici (come il software più diffuso « PGP », realizzato negli anni Novanta dal crittografo statunitense Philip R. Zimmermann) sono stati creati allo scopo di garantire la sicurezza delle comunicazioni tra singoli utenti avvalendosi della stessa tecnologia, ma possono essere utilizzati anche per firmare i documenti: chi spedisce, di norma, cifra il documento con la propria chiave privata prima di utilizzare la chiave pubblica del destinatario per spedire il documento; cosicché chi riceve il messaggio utilizza la chiave privata in suo possesso per « aprire » l'involucro digitale e utilizza, poi, la chiave pubblica del mittente per verificare l'autenticità della firma.

[63] Per adeguare le regole tecniche alle

5. Efficacia sostanziale e valore probatorio delle scritture informatiche.

Le diverse tipologie di firme elettroniche condizionano l'efficacia della scrittura informatica[64], tanto sotto il profilo della forma quanto quella della prova.

Sul piano sostanziale, si distinguono le scritture informatiche che devono essere sottoscritte, a pena di nullità, attraverso una firma elettronica qualificata o digitale per soddisfare la forma scritta *ad substantiam* contemplata dall'art. 1350, nn. 1-12, cod. civ.; le scritture riconducibili all'articolo 1350, numero 13, cod. civ., per le quali il requisito della forma scritta *ad substantiam*, s'intende soddisfatto dai documenti informatici sottoscritti con firma elettronica avanzata, qualificata o digitale (*ex* art. 21 comma 2/*bis*, CAD); tutte le altre scritture informatiche, in cui la forma scritta è richiesta esclusivamente *ad probationem*, per le quali è possibile utilizzare ogni tipo di firma, ferma restando la possibilità per il legislatore di prevedere una disciplina diversa che regoli in maniera alternativa i requisiti e la rilevanza della forma scritta[65] e, conseguentemente, delle scritture informatiche (art. 1325, n. 4, cod. civ.).

La novella del 2012, con il nuovo inciso inserito nel testo dell'art. 21, comma 2, ha quindi consentito di associare anche la firma avanzata (non munita di certificato o non basata su una coppia di chiavi asimmetriche) a tutti « gli altri atti » che necessitano della forma scritta a pena di nul-

modifiche introdotte nel codice dal D.Lgs. 30 dicembre 2010, n. 235, è da tempo in preparazione il testo di nuove regole tecniche sulla firma digitale, firma elettronica qualificata e firma elettronica avanzata. Il 14 maggio 2012 è stata completata la procedura di notifica alla Commissione Europea e agli altri Stati membri. La bozza delle nuove regole tecniche in corso di approvazione, comunque, conferma i principi esposti nel testo (artt. 9 ed 11 del testo pubblicato dall'Agenzia per l'Italia digitale e reperibile all'indirizzo *http://www.digitpa.gov.it/codice-amministr-digitale/attuazione-del-cad*, verificato il 5 marzo 2013).

64 Il riferimento alla scrittura informatica porta, volutamente, a non considerare il valore giuridico e probatorio del mero documento informatico (non sottoscritto), per il quale l'art. 20, comma 1, CAD fissa il criterio generale, secondo cui « l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed inunodificabilità, fermo restando quanto disposto dall'articolo 21 ». Secondo la citata formulazione, introdotta con la novella del 2010 che ha inserito il nuovo comma 1-*bis*, sono soggetti al libero apprezzamento del giudice tanto il profilo sostanziale dei requisiti di forma quanto quello probatorio del documento, fermo restando che per il documento informatico sottoscritto vale la diversa disciplina di cui al richiamato art. 21. Pertanto, l'efficacia probatoria del documento dipende, in primo luogo, dalla circostanza che il medesimo sia munito di firma elettronica, e, successivamente, dal tipo di firma elettronica in concreto utilizzata. Peraltro, le caratteristiche di « qualità, sicurezza, integrità ed immodificabilità » richiamate, oltre che dall'art. 20, anche dall'art. 21, quale parametro per la valutazione giudiziale, sono proprio quelle che si intendono garantite dalla presenza di una firma elettronica avanzata, a fronte della quale la libera valutazione del giudice, viene meno.

65 Non è possibile affrontare, in questa sede, anche il tema dell'idoneità del documento informatico a soddisfare il requisito della forma scritta, sul quale si rinvia a A. Gentili, *Documento elettronico: validità ed efficacia probatoria*, in R. Clarizia (a cura di), *I contratti informatici*, p. 141 ss.; Id., *I documenti informatici: validità e inefficacia*, in *Diritto dell'Internet*, 2006, p. 297 ss.; C. Sandei, *Valore formale e probatorio del documento informatico alla luce del D.Lgs. 4 aprile 2006*, n. 159, in *Nuove leggi civ. comm.*, 2008, p. 15 ss.

lità, completando il regime tipico di tale sottoscrizione, a cui la modifica introdotta con il D.Lgs. 235/2010 aveva già esteso l'efficacia di scrittura privata dell'art. 2702 cod. civ.[66].

Tuttavia, il connotato sostanziale esclusivo delle firme qualificate e digitali, le uniche in grado di soddisfare i requisiti di forma di cui all'art. 1350, nn. 1-12, cod. civ. (*ex* art. 21, comma 2-*bis*, CAD), trova riscontro, anche sul piano probatorio, nella misura in cui solo per esse vige la presunzione di riconducibilità al titolare del dispositivo di firma[67].

Tutti gli altri segni elettronici di identificazione, compatibili con la nozione di firma elettronica, possono essere, invece, validamente apposti solo su scritture informatiche rilevanti quali mezzi di prova e sono comunque rimessi al libero apprezzamento del giudice « tenuto conto delle [...] caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità » (art. 21, 1 comma, CAD)[68].

Sotto il profilo dell'efficacia probatoria, dunque, l'art. 21 del codice dell'amministrazione digitale offre solo due opzioni.

Il documento informatico cui è apposta una firma elettronica c.d. semplice (o « debole »[69]) è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità[70].

Pur trattandosi dello stesso regime previsto per il documento informatico privo di sottoscrizione dall'art. 20, comma 1-*bis*, CAD, sembra corretto ritenere che la presenza di una firma elettronica, per quanto « semplice », sia sufficiente ad assicurare l'utilizzabilità del mezzo di prova, attribuendo al documento un maggior grado di affidabilità e restringendo l'ambito di discrezionalità connesso alla libera valutazione del giudice.

66 Prima della legge 221/2012 la firma elettronica avanzata non risultava direttamente collegata ai requisiti di forma di cui all'art. 1350 cod. civ.

67 Vedi § 6, per l'importanza che esso rivela centrale ai fini del riconoscimento/disconoscimento della sottoscrizione, su cui ci si soffermerà più avanti.

68 Secondo F. Ricci, *Firma digitale*, cit., p. 787, le scritture su cui è apposta una firma elettronica avanzata si porrebbero in posizione intermedia tra le scritture munite di firme elettroniche qualificate e digitali (riconducibili al concetto di « scritture forti ») e quelle munite di firme elettroniche semplici (riconducibili al concetto di « scritture deboli »); sicché andrebbero distinte le scritture informatiche « fortissime », munite di firme elettroniche qualificate o di firme digitali dalle scritture « forti », munite di firma elettronica avanzata e « qualificate » solo sul piano probatorio, e scritture « deboli », munite di firma elettronica semplice. Tale classificazione, che non tiene conto dell'ultima modifica dell'art. 21 del CAD, pone bene in luce la disomogenea efficacia delle diverse firme elettroniche come conseguenza delle continue modifiche del quadro normativo di riferimento. Per una ricognizione delle diverse classificazioni proposte, si veda anche F. Ricci, *Scritture private e firme elettroniche*, cit., pp. 6-10.

69 In dottrina si è soliti distinguere tra scritture « forti » — dichiarazioni sottoscritte con firma chirografa ed autografa dell'autore idonee — a soddisfare la forma scritta di cui agli artt. 1350, 1-12, cod. civ ed aventi l'efficacia probatoria di cui all'art. 2702 cod. civ., e scritture « deboli », idonee a soddisfare requisito di forma previsti da disposizioni diverse dall'art. 1350, nn. 1-12, cit., e rimesse, sul piano probatorio, al prudente apprezzamento del giudice. Tale dicotomia è spesso riproposta anche per le firme elettroniche e firme elettroniche avanzate, in grado di differenziare l'efficacia della relativa scrittura informatica, ma potrebbe risultare fuorviante nella misura in cui le firme elettroniche non hanno la funzione dichiarativa che è propria delle firme avanzate e quindi non appaiono un *minus* di genere bensì uno strumento che assolve ad una diversa funzione.

70 I due ultimi parametri, « integrità e immodificabilità », sono stati aggiunti al CAD dalla novella del 2006.

L'effettivo valore probatorio di un documento informatico, sottoscritto utilizzando un sistema non riconducibile allo schema della firma avanzata (che impiega, ad esempio, la tecnologia RSA senza richiedere la certificazione o l'uso di mezzi sui quali il firmatario può mantenere un controllo esclusivo[71]), sarà così determinato dal giudice di volta in volta, anche mediante il ricorso a presunzioni semplici, valutando le « caratteristiche oggettive » di sicurezza ed integrità e, quindi, il grado di affidabilità che è possibile attribuire agli strumenti di identificazione informatica impiegati dal sistema.

In altri termini: se, da un lato, la presenza della firma elettronica impedisce di negare *in toto* l'efficacia del documento[72], le minori caratteristiche di sicurezza, rispetto ad una firma associata a chiavi certificate e all'uso della *smartcard*, non consentono, pur in assenza di disconoscimento, di attribuire al documento prodotto in giudizio « piena prova », fino a querela di falso, della provenienza delle dichiarazioni di chi l'ha sottoscritto.

Dopodiché è evidente che tanto l'espressa esclusione dell'efficacia probatoria prevista *ex* art. 2702 cod. civ., con conseguente libera valutazione del giudice secondo i criteri descritti dall'art. 21, 1 comma, CAD, quanto la funzione tendenzialmente identificativa di questo tipo di firme[73], rendono inapplicabili le norme processuali sul riconoscimento o il disconoscimento della sottoscrizione al documento munito di firma elettronica « semplice », quali attività tendenzialmente irrilevanti per definirne il valore probatorio[74].

Quanto, invece, all'efficacia probatoria del documento informatico sottoscritto con firma digitale, il legislatore ha scelto sin dalla prima ora[75] il rinvio all'art. 2702 cod. civ., strutturando su di esso la fattispecie della « scrittura privata informatica » quale nuova figura di prova legale[76] da rendere equivalente alla scrittura privata tradizionale.

La firma digitale, infatti, offre obiettive e rilevanti garanzie in termini di sicurezza ed affidabilità della prova.

71 Si vedano i programmi informatici cui s'è fatto cenno al § 4. C'è da chiedersi, tuttavia, dopo la modifica dell'art. 21, che ha fatto perdere alla firma digitale il riferimento allo strumento di firma, se la generazione di una firma crittografica attraverso il software PGP non possa oggi rientrare tra le firme elettroniche « avanzate », considerando il dispositivo informatico personale (il PC, il *tablet*, lo *smartphone*) come il « mezzo » sul quale il firmatario può conservare un controllo esclusivo (secondo la definizione dell'art. 1, lett. *q-bis*, CAD) e la tecnologia RSA come idonea a garantire sia il collegamento ai dati del documento sia la connessione univoca col firmatario.

72 Come invece potrà fare a fronte di un documento informatico non sottoscritto, se ritenuto del tutto privo di quelle caratteristiche oggettive cui la legge si riferisce. In questo senso, si veda anche F. ROTA, *Il documento informatico*, cit., p. 754.

73 *Supra*, § 4.

74 Analogamente G. VERDE, *Prove nuove*, in *Riv. dir. proc.*, 2006, p. 42 ss.; F. RICCI, *Scritture private e firme elettroniche*, cit., pp. 123 ss. In senso contrario C.M. BIANCA, *La firma elettronica: si apre un nuovo capitolo*, cit., p. 1433.

75 Sin dalla previsione introdotta con l'art. 5, comma 1, del regolamento n. 513 del 1997.

76 Prima dell'avvento della firma digitale, la dottrina tendeva a ricondurre anche il documento che si presentava come « scrittura » alla categoria delle riproduzioni meccaniche di cui all'art. 2712 cod. civ.; Si veda MONTESANO, *Sul documento informatico*, cit., p. 1 ss.; G. VERDE, *Per la chiarezza di idee in tema di documentazione informatica*, in *Riv. dir. proc.*, 1990, p. 715 ss.; G.F. RICCI, *Aspetti processuali della documentazione informatica*, in *Riv. trim. dir. proc. civ.*, 1994, p. 863 ss.; S. PATTI, *Della prova documentale*, in *Commentario al Codice Civile*, Bologna, 1996, p. 25 ss.

Innanzitutto, il meccanismo crittografico rende quasi impossibile la contraffazione della firma, in virtù della procedura informatica di validazione che, partendo dalla chiave pubblica che accompagna il certificato (o comunque resa disponibile dal certificatore) consente di accertare se il titolare della chiave privata, usata per firmare, è colui che appare come autore del documento; il che significa individuare con certezza, in caso di esito positivo della validazione, il titolare della chiave privata con cui la firma digitale è stata apposta[77].

Inoltre, l'eventuale esito negativo del processo di verifica consente di evidenziare, e rendere riconoscibile, qualsiasi successiva manipolazione o alterazione del documento su cui la firma digitale è apposta[78].

Sul punto, tuttavia, la dottrina ha offerto due contrastanti interpretazioni del richiamo alla disciplina codicistica e due diverse ricostruzioni dell'efficacia attribuibile al documento munito di firma digitale[79].

Secondo alcuni, il richiamo all'art. 2702 cod. civ. comporterebbe un rinvio integrale alla disciplina dell'efficacia probatoria della scrittura privata, con la conseguenza che l'assoggettabilità della scrittura informatica all'efficacia di piena prova richiederebbe che ad essa, così come alla scrittura privata, non sia opposto un mancato riconoscimento o l'esito negativo di un giudizio di verificazione[80].

Secondo altri[81], invece, si tratterebbe di un rinvio alla sola efficacia descritta dall'art. 2702 cod. civ.; sicché il documento informatico, per il solo fatto di essere firmato con firma digitale (qualificata o avanzata), avrebbe fin da subito l'efficacia di scrittura privata legalmente riconosciuta[82].

[77] In origine, l'art. 1 D.P.R. n. 513/1997 definiva la stessa firma digitale come «il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata» e la chiave pubblica come «l'elemento della coppia di chiavi (...) con il quale si verifica la firma digitale».

[78] A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 1998, p. 441 ss., sp. 509.

[79] Per S. Patti, *La sottoscrizione del documento informatico: la firma digitale*, in *Studi e materiali. Quaderni trimestrali del Consiglio Nazionale del Notariato: La sicurezza giuridica nella società dell'informazione*, Suppl. n. 1, 2008, p. 127 ss., ricostruisce tale diatriba attraverso la contrapposizione tra una ricostruzione «debole» ed una «forte» dell'efficacia probatoria del documento informatico.

[80] Così, F. De Santis, *La disciplina normativa del documento informatico*, cit., p. 392 ss.; F. Ferrari, *La nuova disciplina del documento informatico*, in *Riv. dir. proc.*, 1999, p. 146 ss.; S. Patti, *L'efficacia probatoria del documento informatico*, cit., p. 73; F. Ricci, *Scritture private*, cit., p. 51 ss.; U. Romano, *Firma digitale*, *Digesto civile - Aggiornamento*, Torino 2000, p. 386 ss., sp. 388; G. Verde, *Prove nuove*, cit., p. 44.

[81] In tal senso C.M. Bianca, *I contratti digitali*, in *Studium juris*, 1999, p. 1037; L.P. Comoglio, *Le prove civili*, Milano 2000, p. 549; G. Finocchiaro, *Documento informatico*, cit., p. 982, ss.; A. Gentili, *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ.*, 1998, II, p. 163 ss.; A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 1998, p. 514 ss.; M. Taruffo, *Parola scritta e parola informatica nel processo civile*, in Aa.Vv., *Scrittura e diritto*, Milano, 2000, p. 93 ss.

[82] Come osservato nel § 2, sp. nota 19, la possibilità di ricollegare al documento informatico l'efficacia della scrittura privata, anche in mancanza di riconoscimento espresso o tacito, parve accolta in passato dallo stesso legislatore con la modifica dell'art. 10 del D.P.R. n. 445/2000, operata dall'art. 6 del D.Lgs. n. 10/2002, che eliminò il richiamo all'art. 2702 cod. civ., riconoscendo al documento efficacia di «piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritto».

In realtà, il tema su cui si innerva tale contrapposizione è sempre quello dell'applicabilità delle norme relative al disconoscimento ed alla verificazione (artt. 214 e ss., cod. proc. civ.) alla scrittura informatica; sicché è su questo problema che si concentreranno, tenendo conto delle diverse modalità attraverso le quali si determina la paternità del documento, le considerazioni finali.

6. Disconoscimento e verificazione della scrittura privata informatica.

Ai sensi dell'art. 21, 2 comma, CAD, le scritture informatiche munite di una firma elettronica avanzata, qualificata o digitale fanno tutte « 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 » (art. 2702 cod. civ.).

Il riconoscimento della firma apposta su un documento prodotto in giudizio contro il suo autore ha valore dirimente in ordine alla formazione della (piena) prova sulla provenienza delle dichiarazioni ivi contenute, poiché impone al giudice di prendere atto che l'autenticità della firma è un fatto non controverso e che, pertanto, non è necessario procedere ad alcuna verificazione della scrittura privata (sia essa chirografa o informatica).

Quanto, invece, alla sottoscrizione « legalmente considerata come riconosciuta », occorre far riferimento, per le scritture informatiche, all'art. 25 del CAD[83] e alla c.d. « firma autenticata » dal notaio o da altro pubblico ufficiale a ciò autorizzato (firma che si ha per riconosciuta *ex* art. 2703 cod. civ.) ovvero nel caso in cui l'autore dello scritto non abbia disconosciuto espressamente la sottoscrizione nella prima udienza, o nella prima difesa, successiva alla produzione del documento *ex* art. 215 cod. proc. civ.).

In particolare, scopo dell'autenticazione della firma digitale, qualificata o avanzata, è quello di fornire, attraverso l'attestazione del pubblico ufficiale, la prova legale dell'effettivo utilizzo del dispositivo di firma ad opera del titolare; prova che, diversamente, sarebbe regolata dalla presunzione dell'uso del dispositivo, superabile dalla « prova contraria » rimessa al titolare della firma dall'art. 21, comma 2, del CAD.

Ne consegue che, come per i documenti sottoscritti con firma autografa autenticata dal pubblico ufficiale, solo la querela di falso può condurre all'accertamento di una falsa dichiarazione resa dal notaio[84]; la qual cosa è

[83] L'art. 25, comma 2, D.Lgs. 82/2005 prevede che « L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico ».

[84] Vale a dire il vero e proprio falso ideologico; cfr. F. Ferrari, *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc. civ.*, p. 415 ss., sp. 428; A. Graziosi, *Documento informatico*, cit., p. 501; F. Rizzo, *Il documento informatico*, cit., p.

ben differente dall'accertamento dell'abuso del dispositivo di firma richiesto per disconoscere la scrittura informatica non autenticata.

L'accertamento giudiziale dell'autenticità di una sottoscrizione, operata attraverso la verificazione a seguito di disconoscimento (artt. 214 ss. cod. proc. civ.), ha efficacia analoga al riconoscimento e all'autenticazione.

Molte, tuttavia, sono le argomentazioni critiche sollevate dalla dottrina rispetto alla possibilità di applicare tale schema alle firme elettroniche avanzate, qualificate e digitali, apposte sulle scritture informatiche.

Secondo alcuni autori, come detto, il ricorso ad un dispositivo per la creazione della firma (artt. 32 e 35 CAD), interposto tra la volontà di apporre la sottoscrizione e la produzione del codice cifrato che costituisce la firma qualificata o digitale, renderebbe queste firme indistinguibili dalla volontà del titolare; con la conseguenza che la procedura di verificazione diverrebbe impossibile, perché potrebbe dimostrare solo l'utilizzo del dispositivo per generare quella firma, ma non anche l'effettivo uso dello stesso strumento da parte del suo titolare (che potrebbe aver consentito ad altri di sottoscrivere il documento al suo posto)[85].

Considerata, dunque, l'impossibilità di considerare la firma digitale, apposta da un soggetto diverso dal titolare dello strumento di firma, come una firma « falsa » (in quanto essa sarebbe sempre il prodotto della cifratura del testo con la chiave privata del titolare), per superare la prova della provenienza del documento, e avvalorare l'illecito utilizzo del dispositivo di firma da parte di terzi, non resterebbe, dunque, che ricorrere alla querela di falso[86].

306; A. GENTILI, *Documento elettronico: validità ed efficacia probatoria*, cit., p. 158 ss.; M. ORLANDI, *Il falso digitale*, Milano, 2003, p. 139.

[85] C.M. BIANCA, *La firma elettronica*, cit., p. 1433; G. FINOCCHIARO, *La firma digitale*, cit., p. 120 ss.; ID., *Firma digitale e firme elettroniche*, Milano 2003, p. 122 ss.; A.M. GAMBINO, *Firma digitale*, cit., *passim*; A. GENTILI, *Documento informatico e tutela dell'affidamento*, cit., p. 173; ID., *Documento elettronico: validità ed efficacia probatoria*, cit., p. 141 ss.; M. ORLANDI, *Commento all'art. 10*, in *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, cit., p. 755 ss. Analoga sembra la posizione di CALZOLAIO, *L'imputazione della dichiarazione nel documento informatico tra volontà e affidamento: spunti per una riflessione*, in *Riv. trim. dir. proc. civ.*, 2005, p. 937, per il quale la scrittura privata « elettronica » disconosciuta dall'apparente sottoscrittore potrebbe, comunque, essere ritenuta attendibile e quindi valutata sul piano probatorio dal giudice. Tale posizione, tuttavia, non sembra più sostenibile dopo le modifiche apportate dal 2006, ulteriormente dettagliate e razionalizzate con le novelle del 2010 e del 2012, all'art. 21, comma secondo, oltre che alle altre norme del medesimo capo del D.Lgs. n. 82/2005. In particolare essa suona difficilmente conciliabile con la possibilità di ottenere l'autenticazione di ogni firma elettronica *ex* art. 25 CAD, che descriverebbe un opzione inutile se il documento sottoscritto con firma elettronica avanzata, qualificata o digitale, nascesse già munito dell'efficacia di prova legale che l'autenticazione è in grado di conferirgli.

[86] Oltre agli autori già citati, si vedano F. RIZZO, *Il documento informatico*, cit., p. 231 ss. e F. VIGLIONE, *L'imputazione dei documenti*, cit., p. 258 ss. Di contrario avviso A. GRAZIOSI, *Documento informatico*, cit., p. 501, che osserva come, essendo la querela di falso strumento, ultimo e necessario, cui ricorrere per impugnare un documento con firma (digitale) autenticata, la scrittura informatica munita di una comune firma avanzata debba godere di una presunzione *juris tantum*, a cui il titolare della firma (digitale, qualificata o avanzata) può reagire senza dover instaurare un autonomo giudizio di falso, ma semplicemente fornendo al giudice, nell'ambito del medesimo processo, la prova di non aver utilizzato il dispositivo di firma. Analogamente, si veda M.G. SCARPA, *Le nuove frontiere dell'efficacia probatoria del documento informatico*, in *Riv.*

Secondo altri, invece, la presunzione legale di utilizzo del dispositivo da parte del titolare, e la conseguente inversione dell'onere probatorio a carico di quest'ultimo, indurrebbero a ritenere il documento informatico comunque dotato di un'efficacia probatoria superiore a quella assegnata alla scrittura privata tradizionale; ciò che impedirebbe l'applicazione della disciplina del disconoscimento e della successiva verificazione o, comunque, porterebbe a delineare un procedimento di verificazione difforme (ed estraneo) rispetto a quello riservato alla tradizionale scrittura privata[87].

La tesi che qui si intende sostenere, invece, prende le mosse dallo *status* di prove critiche precostituite, che è proprio delle firme elettroniche avanzate (qualificate e digitali), per affermare che è sempre possibile risalire, per mezzo di presunzioni (art. 2727 cod. civ.), dalla *segnatura digitale* della scrittura informatica al suo autore.

Va premesso che, analogamente a quanto avviene per la sottoscrizione autografa, anche per le firme elettroniche avanzate, qualificate o digitali, l'oggetto della verificazione non consiste nel superamento della apparente indistinguibilità esteriore della firma apposta sul documento rispetto ad altra firma che si assume sicuramente « autentica »[88], bensì nell'accertamento della effettiva provenienza del documento dal soggetto che figura come suo autore, attraverso un insieme di elementi che per gravità, precisione e concordanza appaiono idonei ad offrire detta prova integrando la presunzione di legge (art. 21, comma 2, CAD).

Occorre, peraltro, distinguere le firme grafometriche (che rientrano nel novero delle firme avanzate) dalle firme qualificate e digitali, per le quali soltanto, come detto, l'utilizzo del dispositivo di firma si presume riconducibile al titolare (*ex* art. 21, comma 2, CAD).

La firma digitale fonda le proprie garanzie di sicurezza, integrità ed autenticità proprio sulla possibilità di verificazione informatica (validazione) della sottoscrizione; cioè sulla possibilità, offerta dal sistema crittografico a chiavi asimmetriche, di risalire dalla chiave pubblica che accompagna il certificato alla chiave privata con cui il testo è stato cifrato (e queste considerazioni possono estendersi anche alla firma qualificata, nella misura in cui essa si fonda sull'uso di un dispositivo sicuro e sul certificato qualificato). Ma anche la firma grafometrica, come s'è visto, si affida non solo al carattere personalissimo della sottoscrizione autografa, ma anche dei dati biometrici acquisiti durante la firma ed usati come chiave di cifratura per associare la firma al testo.

Sarebbe del tutto incongruente, dunque, considerare la scrittura informatica prodotta in giudizio come idonea ad acquisire efficacia di piena

trim. dir. proc. civ., 2008, p. 260; C. SANDEI, *Valore formale e probatorio*, cit., p. 27; F. FERRARI, *Il codice dell'amministrazione digitale*, cit., p. 425.

[87] Così F. FERRARI, *Il codice dell'amministrazione digitale*, cit., p. 426, il quale peraltro sembra escludere che l'applicabilità dell'art. 2702 cod. civ. valga a richiamare gli artt. 214 ss. cod. proc. civ. Analogamente F. ROTA, *Il documento informatico*, cit., p. 760. Secondo C. SANDEI, *Valore formale e probatorio*, cit., p. 27 ss., sp. 30 sono state così valorizzate dal punto di vista procedurale le differenze strutturali intercorrenti tra firma autografa e firma digitale, adottando un procedimento di « verificazione » *sui generis*, più agevole e maggiormente adeguato alla realtà tecnica dei documenti firmati digitalmente.

[88] Ed infatti, anche nel caso delle scritture tradizionali si è soliti osservare che la piena identità di due firme, porta a considerare una delle due certamente falsa.

prova documentale, *ex* art. 2702 cod. civ., solo quando il firmatario abbia omesso di disconoscerla (o l'abbia espressamente riconosciuta) e non anche quando l'autenticità sia stata accertata a seguito della verifica (informatica) della scrittura.

L'accertamento giudiziale dell'autenticità della firma, com'è noto, è introdotto dall'istanza di verificazione proposta dalla parte interessata a valersi della scrittura disconosciuta e può essere raggiunto con l'ausilio di qualsiasi mezzo di prova utile: tra questi, non può essere ignorata la *verificazione informatica* che, analogamente agli effetti che consegue una perizia grafica, consente di risalire dal segno apposto sullo scritto al suo presumibile autore.

L'art. 21, comma secondo, CAD, stabilendo che la firma elettronica (avanzata, qualificata o digitale) apposta sul documento informatico, per vedersi attribuita l'efficacia prevista dall'articolo 2702 cod. civ., dev'essere formata « 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 », chiarisce anche che non è la titolarità della firma che rileva per la formazione della prova sulla provenienza di una dichiarazione, ma la riconducibilità al titolare del gesto che l'ha generata; vale a dire, nel caso della firma qualificata o digitale, l'utilizzo del dispositivo sicuro per la generazione della firma.

In altre parole, ai fini della paternità della scrittura informatica munita di firma digitale (o qualificata) non basta che su di essa risulti apposta la firma attribuita al titolare del dispositivo, ma è necessario che tale firma sia stata apposta mediante l'utilizzo del dispositivo di firma e con gesto intenzionale del suo titolare[89].

Allo stesso tempo, l'aver precisato che « l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria »[90] ha esplicitato una presunzione che, essendo suscettibile di prova contraria, dovrà poter essere oggetto di accertamento affinché si dimostri il mancato impiego del dispositivo di firma o si formi piena prova dell'avvenuto utilizzo ad opera del titolare.

È la parte contro cui la scrittura informatica è stata prodotta che deve fornire tale prova contraria e dimostrare la non autenticità della sottoscrizione, ma ciò non toglie che la parte che intende valersi del documento debba, comunque, *fornire la prova del concreto utilizzo del dispositivo di firma attribuito al titolare*, non essendo sufficiente la mera esibizione della scrittura informatica.

Si tratta di una prova agevole, di norma offerta dal certificatore con l'attestato digitale (art. 1 lett. *e* ed *f* CAD) che accompagna il documento e con la « certificazione » che la chiave utilizzata per firmare appartiene ad una coppia generata dal dispositivo attribuito al firmatario (il quale, peraltro, dev'essere « identificato con certezza », *ex* art. 32, comma 3, lett. *a* CAD, dal certificatore che emette certificati qualificati).

[89] Non a caso, infatti, l'allegato III della direttiva 99/93/CE sulle firme elettroniche prevede che i dispositivi sicuri per la creazione della firma presentino i dati da firmare « ...al firmatario prima dell'operazione di firma ».

[90] Così l'art. 21, comma secondo, D.Lgs. 82/2005 come modificato da ultimo dal D.Lg. n. 235/2010.

Com'è noto, la firma digitale si compone di una stringa di caratteri che non è immediatamente intellegibile, essendo il prodotto della cifratura di una stringa rappresentativa del testo mediante la chiave privata, sicché essa non appare immediatamente riconducibile al suo autore. Solo riconducendo la firma al dispositivo che l'ha generata è possibile arrivare all'autore e, secondo quanto dispone l'art. 216 cod. proc. civ., tale relazione dev'essere ricostruita attraverso « i mezzi di prova che [chi chiede la verificazione] ritiene utili... »[91].

In altre parole, a fronte di una scrittura informatica sottoscritta con firma digitale (o qualificata), anche la parte che intenda veder confermata la bontà della firma può valersi, oltre che di presunzioni semplici, della procedura di verificazione informatica.

Peraltro, l'accertamento di autenticità così ottenuto è necessario e sufficiente affinché operi la presunzione di riconducibilità al titolare (*ex* art. 21, 2 comma, CAD) e si formi la prova piena della integrità, genuinità ed immodificabilità del documento, fino a querela di falso (*ex* artt. 21, comma 2, CAD e 2702, cod. civ.)[92].

Se, pertanto, l'onere probatorio imposto alla parte che richiede la verificazione appare piuttosto agevole, resta da chiarire su cosa debba vertere la contro-prova richiesta alla parte che ha operato il disconoscimento. E, per farlo, occorre tornare sulla presunzione che tale prova contraria è chiamata a superare.

La presunzione di affidabilità della prova (l'essenza di ciò che è prova critica precostituita) è basata, nel caso della firma digitale (o qualificata), sull'apprezzamento delle caratteristiche del dispositivo impiegato per la generazione e la validazione delle firme, mentre quella propria delle firme autografe (e, per certi versi, delle firme grafometriche) s'innerva sulla peculiarità dei segni e caratteri impressi sul documento dal singolo e sulla verifica di compatibilità con quelli propri della firma usualmente apposta dal medesimo.

Tale differenza condiziona il diverso passaggio logico che consente di pervenire dal segno al suo autore e, quindi, alla titolarità della sottoscrizione; come detto, se per le firme tradizionali esso poggia sulla comparazione tra firme attuali e precedenti, per la firma digitale (o qualificata) sarà, invece, necessario procedere alla verificazione informatica (c.d. *validazione*) della sottoscrizione da attribuire.

Occorre tener presente, peraltro, che l'apposizione sullo scritto della firma autografa (o di quella grafometrica, che viene generata allo stesso modo) è un gesto che deve essere compiuto necessariamente dal firmatario,

[91] Oltre che « ... producendo o indicando le scritture che possono servire di comparazione », elementi, come detto, di nessuna utilità nel caso di specie poiché estranei alla relazione tra la firma elettronica ed il suo autore. Diversamente, rispetto alle firme elettroniche ed all'uso abusivo dello strumento di firma potrebbe, invece, rendersi necessario identificare il dispositivo che è stato utilizzato per formare il documento, la chiave privata utilizzata per apporre la firma, il percorso seguito dal documento trasmesso per via telematica, la validità del certificato emesso dal soggetto certificatore ed altre simili attività che richiedono il ricorso ad accertamenti tecnici complessi e senz'altro più onerosi della semplice acquisizione e produzione di scritti di comparazione.

[92] Quanto al modo sostanzialmente analogo, in cui la presunzione di autografia della firma chirografa contribuisce alla formazione della prova sulla provenienza della dichiarazione *ex* art. 2702 cod. civ. vedi V. DENTI, *La verificazione delle prove documentali*, Torino, 1957, p. 29 ss.

mentre, nel caso delle firme elettroniche qualificate e digitali, il gesto può anche essere materialmente compiuto da un soggetto diverso da quello indicato dalla firma, senza che questo impedisca al codice cifrante di formarsi e di legarsi inscindibilmente al testo.

Muta, pertanto, la modalità d'interposizione del terzo rispetto alla corretta apposizione del segno di firma e, conseguentemente, la prova contraria che il disconoscente è chiamato ad offrire al fine di superare la presunzione di riconducibilità dell'utilizzo del dispositivo di firma al suo titolare: detta prova non risiede nella circostanza che la firma è stata apposta da un terzo, bensì nella dimostrazione che ciò è avvenuto al di fuori della sfera di controllo del titolare del dispositivo.

Posto che la dimostrazione del fatto negativo (l'omessa sottoscrizione) non si sottrae all'ordinario riparto dell'onere probatorio ed è pacificamente ammessa dalla giurisprudenza della Corte di cassazione[93], il caso più evidente è offerto dalla prova della perdita incolpevole dello strumento di firma, da parte del suo titolare, prima della sottoscrizione del documento, attraverso la produzione in giudizio della denuncia di furto o smarrimento seguita dalla tempestiva notifica al fornitore del servizio per la revoca del certificato.

Tuttavia, anche nel caso in cui il titolare abbia accertato l'uso abusivo dello strumento di firma da parte di soggetti non autorizzati senza denunciare la perdita del possesso, l'accertamento del giorno, dell'ora e del luogo in cui è stata apposta una firma digitale (o qualificata) senza il consenso del titolare è comunque favorito dalle disposizioni regolamentari che impongono all'utente ed ai fornitori dei servizi, connessi con l'uso di queste firme, una continua attività di registrazione e trascrizione in repertorio delle operazioni; sicché la prova che la firma non può essere stata apposta su un determinato documento da chi, al momento della formazione dell'atto, si trovava con certezza in altro luogo, è sempre possibile.

È evidente che il consulente tecnico, eventualmente chiamato ad assistere il giudice nella verificazione di questo tipo di firme, non può essere un perito calligrafico, ma dev'essere scelto tra gli esperti nelle materie informatiche; così come è evidente che la perizia (ad eccezione del caso della firma grafometrica) non avrà ad oggetto precedenti sottoscrizioni effettuate col medesimo strumento di firma, bensì elementi che descrivano le abituali modalità di utilizzo del dispositivo (dai quali possa evincersi qualche sostanziale differenza rispetto al documento disconosciuto): tipicamente, l'uso di una macchina informatica diversa da quella abitualmente adoperata per sottoscrivere documenti dello stesso tipo, o l'invio a distanza del documento utilizzando indirizzi IP o percorsi diversi.

[93] Secondo la suprema Corte, l'onere della prova gravante su chi intende far valere in giudizio un diritto, ovvero su chi eccepisce la modifica o l'estinzione dei diritto da altri vantato, non subisce deroghe nemmeno quando abbia ad oggetto « fatti negativi », in quanto la negatività dei fatti oggetto della prova non esclude né inverte il relativo onere; tuttavia, non essendo possibile la materiale dimostrazione di un fatto non avvenuto, la relativa prova può essere data mediante dimostrazione di uno specifico fatto positivo contrario, od anche mediante presunzioni dalle quali possa desumersi il fatto negativo. Cfr. Cass., sez. V, 6 giugno 2012, n. 9099. Conformi: Cass., sez. I, 8 ottobre 2008, n. 24865; Cass., sez. lav., 9 giugno 2008, n. 15162; Cass., sez. III, 11 gennaio 2007, n. 384; Cass., sez. III, 1 novembre 2003, n. 17146; Cass., sez. V, 15 aprile 2002, n. 5427; Cass., sez. lav., 14 luglio 2000, n. 9385.

Anche per la verificazione di scrittura privata informatica, inoltre, è sempre possibile ammettere ai sensi dell'art. 217 cod. proc. civ., oltre alla consulenza tecnica, « altre prove » ritenute rilevanti per la dimostrazione della falsità dello scritto informatico o disporre l'accesso « presso depositari pubblici o privati » per prelevare documenti che non si trovano nella disponibilità della parte istante.

La ricostruzione sin qui tratteggiata, nel condurre ad una piena applicabilità dello schema disconoscimento-verificazione descritto dal codice di procedura civile, consente anche di superare la diversa lettura secondo cui, nel sistema delineato dall'art. 21 del CAD, la sottoscrizione del documento sarebbe sempre riconducibile, anche nel caso di falsificazione della firma, alla persona che è titolare della coppia di chiavi, essendo la firma digitale (come ogni altra firma avanzata) un mero « sigillo » apposto al testo con un sistema di cifratura[94]. Per questa via, infatti, non avrebbe senso proporre un vero e proprio disconoscimento endo-processuale della scrittura informatica, potendo il titolare dello strumento di sottoscrizione far soltanto valere la falsità della scrittura attraverso la querela di falso[95].

Si tratta di una soluzione radicale che non appare condivisibile; se non altro perché essa conduce inevitabilmente all'esclusione, per gli stessi motivi, anche dell'esperibilità di un'azione di disconoscimento proposta in via principale, *ex* art. 216 cod. proc. civ. — vale a dire di un'azione che abbia come oggetto specifico l'accertamento della falsità della sottoscrizione — con l'incongruo risultato di rendere il documento informatico obiettivamente munito di un'efficacia probatoria « rafforzata » rispetto al documento formato su supporto cartaceo. Approdo, quest'ultimo, che sarebbe palesemente in contrasto con gli obiettivi della direttiva 1999/93/CE — di cui le norme del codice dell'amministrazione digitale costituiscono, per la parte che riguarda le firme elettroniche, norme di recepimento[96] — estranei all'idea che l'efficacia probatoria di un documento informatico munito di firma digitale possa essere maggiore di quella attribuita ad una scrittura privata con sottoscrizione autografa.

[94] Cfr. G. FINOCCHIARO, *Ancora novità legislative in materia di documento informatico:...*, cit., p. 502: secondo cui « [...] La scrittura informatica è, infatti, impersonale e priva di grafia e l'apposizione della firma digitale non è, per sua stessa natura, un gesto personalissimo della mano del sottoscrittore. ». Analogamente, sul valore metaforico che l'impiego del termine « firma » assume nel contesto del documento informatico, poiché estranea alla tradizionale sottoscrizione autografa, si veda G. FINOCCHIARO, *La firma digitale*, cit., p. 1 ss.; ID., *Tecniche di imputazione della volontà negoziale; le firme elettroniche e la firma digitale*, in R. CLARIZIA (a cura di), *I contratti informatici*, Torino, 2007, p. 203.

[95] Per G. FINOCCHIARO, *Ancora novità legislative*, cit., p. 502: « Si può dunque affermare che la particolare natura tecnologica della firma digitale e del documento informatico hanno condotto all'elaborazione di una nuova tipologia di disconoscimento, che non ha ad oggetto né la sottoscrizione né la scrittura, caratteristiche esteriori del documento informatico, ma esclusivamente l'utilizzo del dispositivo di firma. Si passa da un criterio di "paternità" ad un criterio di "responsabilità" [...] ».

[96] Le norme del CAD, come si è avuto modo di osservare (vedi § 2) replicano, integrano e modificano le norme del discusso D.Lgs. 23 gennaio 2002, n. 10 di recepimento della direttiva 1999/93/CE sulle firme elettroniche, laddove la delega contenuta nell'articolo 10 della legge 29 luglio 2003, n. 229 (« Riassetto in materia di società dell'informazione ») prevedeva espressamente, alla lettera *e*), l'adeguamento della normativa da riordinare alle disposizioni comunitarie. Peraltro, nell'epigrafe del C.A.D. è contenuto un riferimento espresso al D.Lgs. 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE.

Le disposizioni sovranazionali, al contrario, impongono agli Stati membri dell'Unione di attribuire alle firme elettroniche « i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei », il che conduce a una firma digitale in tutto e per tutto equiparata alla firma autografa[97].

Tali considerazioni, se condivise, rinforzano una volta di più l'opzione in favore del giudizio di verificazione e conducono a definirne adempimenti e modalità al fine di comprendere in quale momento del giudizio e con quali regole si forma la presunzione di autenticità della sottoscrizione, necessaria perché la scrittura informatica acquisti « l'efficacia prevista dall'art. 2702 cod. civ. ».

Data la complessità e la molteplicità dei criteri e dei modi alternativi per compiere la verificazione informatica, nonché il differente esito che tale verificazione può dare in funzione della modalità prescelta e del momento in cui è compiuta, essa dev'essere necessariamente eseguita in udienza e nel contraddittorio tra le parti interessate[98], escludendo una volta di più che l'efficacia probatoria della scrittura informatica possa essere attribuita per il solo fatto che la scrittura sia venuta ad esistenza o sia stata prodotta in giudizio[99].

La necessità del ricorso alla verificazione giudiziale implica il riferimento ad un procedimento che consenta di controllare la sussistenza di indizi precisi in ordine alla provenienza della sottoscrizione, e, in mancanza di disposizioni di senso contrario, porta a ritenere che la medesima debba seguire le regole dettate dagli artt. 214 ss. cod. proc. civ.

In tal modo, in forza del richiamo alle norme del codice, è fuor di dubbio che chi vi abbia interesse possa proporre istanza di verificazione non solo in via incidentale (cioè in occasione e nei limiti di rilevanza che il documento assume nell'ambito del giudizio), ma anche in via principale (*ex* art. 216, 2 comma, cod. proc. civ.) e nell'ambito di un giudizio autonomo avente ad oggetto l'accertamento dell'autenticità del documento.

Inoltre, in caso di disconoscimento, l'onere di impulso sarà comunque posto a carico della parte interessata a formare la prova della dichiarazione, superando l'apparente inversione di cui all'art. 21, 2 comma, CAD, oltre a consentire a chi produce la scrittura di ottenerne la verificazione attraverso tutti « i mezzi di prova che ritiene utili » e non solo sulla base della verificazione informatica.

Può dirsi, infatti, che la presunzione di cui all'art. 21, 2 comma CAD costituisce il mezzo per riequilibrare l'onere della prova a fronte della maggiore difficoltà cui andrebbe incontro la parte che si vede disconoscere in giudizio il documento informatico su cui fonda la pretesa o l'eccezione, nel procurarsi la prova dell'autenticità del documento.

[97] Attribuendo al documento informatico, munito di firma digitale o qualificata, un'efficacia probatoria maggiore di (o, se si preferisce, diversa da) quella assunta dalla scrittura privata munita di sottoscrizione autografa, per effetto della maggiore difficoltà frapposta dall'ordinamento al disconoscimento della firma digitale, si finirebbe col sostenere, in sostanza, che il decreto delegato per il recepimento della direttiva comunitaria ha ecceduto i limiti imposti dalla legge di delegazione; con la conseguenza che il contrasto con l'ordinamento comunitario, potrebbe risolversi solo con la disapplicazione delle norme interne o attraverso un intervento della Corte Costituzionale.

[98] F. Ricci, *Firma Digitale*, cit., p. 792.

[99] Si veda nota 81.

In altre parole, il legislatore pone l'onere di provare l'assenza del controllo sul dispositivo a carico della parte che ha la disponibilità della prova, in ossequio a quel principio, da molti anni affermato dalla giurisprudenza di legittimità, secondo cui l'onere della prova dev'essere ripartito, oltreché secondo la descrizione legislativa della fattispecie sostanziale controversa, con l'indicazione dei fatti costitutivi e di quelli estintivi o impeditivi del diritto, « ...anche secondo il principio della riferibilità o vicinanza, o disponibilità del mezzo; principio riconducibile all'art. 24 Cost., che connette al diritto di azione in giudizio il divieto di interpretare la legge rendendone impossibile o troppo difficile l'esercizio »[100]. La qual cosa appare del tutto coerente con lo scopo normativo, che è quello di rendere effettivamente equivalente alla scrittura privata, anche con riferimento alle concrete possibilità di difesa in giudizio, il valore probatorio delle scritture informatiche.

Analogamente a quanto avviene per la consulenza grafica, il livello di approfondimento dell'istruttoria è quindi rimesso all'apprezzamento del giudice in ordine agli elementi offerti dalla perizia/verificazione informatica e ad eventuali ulteriori elementi di valutazione (probatori o indiziari); i quali contribuiscono tutti a definire la soluzione più appropriata, sulla base del contemperamento fra le esigenze di economia processuale e la scelta di tecniche di verifica sufficienti a formare presunzioni gravi, precise e concordanti in ordine all'avvenuto utilizzo del dispositivo di firma (art. 2729 cod. civ.), nonché in ordine alla riconducibilità di tale utilizzo al titolare della chiave con cui è stata apposta la firma digitale[101].

Il giudice, se richiesto tempestivamente, può anche ammettere l'eventuale prova contraria, che può essere offerta dalla parte interessata al disconoscimento (art. 21, comma secondo, D.Lgs. n. 82/2005 e 2728 cod. civ.) al fine di contrastare le risultanze della verificazione informatica.

In conclusione, può dirsi che la verificazione della scrittura privata informatica non è un procedimento impossibile, né incompatibile con le disposizioni del codice di rito civile. L'applicazione integrale dell'art. 2702 cod. civ. e degli artt. 214 ss. cod. proc. civ., al contrario, non solo appare più aderente al dato testuale, ma consente il pieno rispetto degli obiettivi dichiarati dal legislatore[102]: garantire l'equivalenza delle scritture autografe e informatiche, evitare il facile ripudio delle scritture informatiche anche da parte di chi ne sia effettivamente l'autore, pur senza imputare forzosamente al titolare della firma quelle scritture che non sono riconducibili alla sua sfera di volontà e di controllo.

[100] Cass., sez. lav., 1 luglio 2009, n. 15406; Cass., sez. lav., 25 luglio 2008, n. 20484; Cass., Sez. Un., 10 gennaio 2006, n. 141; Cass., Sez. Un, 30 ottobre 2001, n. 13533.

[101] Come detto, le soluzioni possibili sarebbero molteplici, ma è lecito escludere che la valutazione del giudice sul formarsi della presunzione si realizzi retrocedendo sino al momento di generazione della firma o di deposito in giudizio del documento che la contiene. Più probabile che il giudice sia chiamato ad ispezionare la firma *off line* applicando ad essa il *software* che ne consente non solo la lettura, ma anche una verificazione di primo livello tramite il repertorio dei certificati memorizzati nel *computer* di colui che sta procedendo all'esame; ovvero a verificarla *on line* consultando una delle copie operative del repertorio dei certificati tenuto dai certificatori o consultando la copia di riferimento contenuta nel registro dei certificatori.

[102] Peraltro, già la direttiva 1999/93/CE sulle firme elettroniche, all'art. 5, richiedeva, per quanto attiene al processo, di non considerare la sottoscrizione « legalmente inefficace e inammissibile come prova in giudizio [...] unicamente a causa del fatto che è in forma elettronica » (art. 5).

Abstract

Starting from the consideration that an electronic document is the written representation of relevant facts used as evidence in legal proceedings, the paper aims to demonstrate the full compatibility of the current regulatory framework (after the changes introduced into the Italian eGovernment Code in 2012), with the disavowal of electronic signatures in the court and with the signature verification procedure provided for in Articles 214 and following of the Italian Code of Civil Procedure, the purpose of which has recently been challenged by many authors.