FRANCESCO RIZZO

VALORE GIURIDICO ED EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO

SOMMARIO: 1. Introduzione. — 2. Rilevanza giuridica del documento informatico. — 3. Efficacia probatoria. — 4. (Segue) scrittura privata informatica e prova legale. — 5. (Segue) presunzione di riferibilità; nuova verificazione. — 6. (Segue) querela di falso. — 7. (Segue) opponibilità.

1. INTRODUZIONE.

Gli sviluppi della tecnologia mai come negli anni attuali hanno aperto, in maniera così rapida e frenetica, nuovi orizzonti alle modalità comunicative che sono, ormai, in grado di superare i consueti limiti imposti dallo spazio e dal tempo.

In questo contesto interessa, in particolare, rilevare che le recenti innovazioni hanno consentito di aggiungere alle tradizionali attività documentative un altro importante mezzo con cui porre in essere dei documenti.

Tutto ciò ha fatto sì che nuovi fenomeni come il commercio elettronico e la documentazione informatica abbiano assunto eccezionale rilevanza nella nostra società, tanto da generare situazioni del tutto nuove ed inconcepibili fino a qualche tempo fa. In questo scenario, attentamente osservato nel frattempo dalla dottrina[1] sollecitata oltre che dalle novità del fe-

[1] La dottrina che si è occupata del documento elettronico prima dell'emanazione della L. 15 marzo 1997, n. 59, è particolarmente ampia. Essa anche prima di tale data giunge in alcuni casi a risultati molto interessanti da un punto di vista giuridico. A riprova di ciò v.: L. ALBERTINI, *Osservazioni sulla conclusione del contratto tramite computers e sull'accettazione di un'offerta in internet*, in *Giust. civ.*, II, 1997, p. 26; R. BORRUSO, *Computer e diritto*, Milano, 1988; ID., *Tre tesi di fondo dell'informatica giuridica*, in *Giur. it.*, 1986, p. 219; R. CLARIZIA, *Informatica e conclusione del contratto*, Milano, 1985; B. DEL VECCHIO, *Riflessioni sul valore giuridico della sottoscrizione elettronica*, in *Riv. not.*, 1991, p. 977; F. DEVESCOVI, *Titoli di credito ed informatica*, Padova, 1991; P.M. DI GIOVANNI, *Il contratto concluso mediante computer alla luce della Convenzione di Roma sulla legge applicabile alle obbligazioni contrattuali del 19 giugno 1980*, in *Diritto del commercio internazionale*, 1981, p. 582; S. FADDA, *L'electronic data interchange nella normativa italiana e straniera*, in questa *Rivista*, 1994, p. 24; G. FINOCCHIARO, *Documento elettronico*, in *Contratto e impresa*, 1994, p. 433; ID., *I contratti informatici*, in *Tratt. di dir. comm. e di dir. pubbl. dell'econ.* diretto da F. Galgano, XXII, Padova, 1997; V. FRANCESCHELLI, *Computer, documento elettronico e prova civile*, in *Giur. it.*, IV, 1998, p. 314; A. GALLIZIA, *Notariato, pubblicità legale e informatica*, in *Notariato*, 1997, p. 445; ID., *Il documento informatico e la sicurezza giuridica*, in *Riv. not.*, 1991, p. 77; A.M.

nomeno anche dalla necessità di individuare le eventuali implicazioni giuridiche, è di recente intervenuto il legislatore.

Questi dopo aver acquisito consapevolezza del problema e della complessità dello stesso ha provveduto a disciplinarlo in maniera diretta, avvalendosi dei suggerimenti della dottrina[2] e delle esperienze maturate in altre nazioni[3], non recepiti passivamente, ma valutati e filtrati in maniera critica.

Il legislatore non ha, così, voluto abbandonare la società di un futuro sempre più vicino ad un sistema privo di regole e di norme giuridiche adatte. Egli, infatti, compreso che le attuali scoperte tecnologiche comportano implicazioni e conseguenze talora dirompenti, non si è arroccato nella « cittadella del diritto »[4] respingendole; con spirito di apertura le ha, in-

---

GAMBINO, *Gli scambi in rete*, in questa *Rivista*, 1997, p. 423; ID., *L'accordo telematico*, Milano, 1997; ID., *Commercio telematico dei beni immateriali*, in *Contratto e impresa*, 1997, p. 710; G. GIACOBBE, *Spunti in tema di disciplina del contratto e tecniche informatiche*, in *Legalità giust.*, 1993, p. 409; E. GIANNANTONIO, *Il valore giuridico del documento elettronico*, in *Diritto del commercio internazionale*, 1991, p. 262; ID., *Manuale di diritto dell'informatica*, Padova, 1994; L. GRISOSTOMI TRAVAGLINI, *Un esempio di EDI: la fattura elettronica*, in *Giur. it.*, IV, 1993, p. 156; N. IRTI, *La memoria dell'impresa (dai quadernacci di Francesco Datini ai nastri magnetici)*, in *Riv. dir. proc.*, 1991, p. 52; A. L. MARCONI, *La legge Modello UNCITRAL sul commercio elettronico*, in *Diritto del commercio internazionale*, 1997, p. 137; M. MICCOLI, *Cybernotary*, in *Notariato*, 1996, p. 1076; G. MIRABELLI, *Contratto tra terminali e documento elettronico*, in *Riv. not.*, 1986, p. 796; A. MIRANDA, *« Surfing contracts » luce nuova sulla conclusione del contratto mediante mezzi elettronici*, in *Vita notarile*, 1996, p. 666; L. MONTESANO, *Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Riv. trim. dir. proc. civ.*, 1987, p. 23; N. SCANNICCHIO, *Consumatori e conclusione di contratti a distanza tra ordinamenti nazionali, direttiva comunitarie e diritto comparato*, in *Riv. crit. dir. priv.*, 1994, p. 3; M. ORLANDI, *La paternità della scrittura*, Milano, 1997, p. 501; F. PARISI, *Il contratto concluso mediante computer*, Padova, 1987; U. PLALANICA, *Regolamento degli acquisti effettuati via internet*, in *Inform. e documentazione*, 1997, p. 81; R. RAGOZZO - D. GIAQUINTO, *Il sigillo informatico*, in *Notariato*, 1997, p. 80; D. REDOLFI, *Reti telematiche e commercio elettronico: la tutela dei consumatori*, in *Il diritto industriale*, 1997, p. 245; G.F. RICCI, *Aspetti processuali della documentazione informatica*, in *Riv. trim. dir. proc. civ.*, 1994, p. 863; F. SFORZA, *Formazione del consenso e strumenti informatici*, in *Contratti*, 1997, p. 89; F. STALLONE, *La forma dell'atto giuridico elettronico*, in *Contratto e impresa*, 1990, I, p. 576; D. SYX, *La firma nei rapporti giuridici elettronici*, in questa *Rivista*, 1993, p. 163; G. VERDE, *Per la chiarezza di idee in tema di documentazione informatica*, in *Riv. dir. proc.*, 1990, p. 715; R. ZAGAMI, *Firme digitali, crittografia e validità del documento elettronico*, in questa *Rivista*, 1996, p. 152.

[2] Vedi nota 1.

[3] Si rileva, infatti, che il primo e più importante regolamento di attuazione si ispira ampiamente a soluzioni straniere e sovranazionali (R. ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente « Atti, documenti e contratti in forma elettronica »*, in questa *Rivista*, 1997, p. 903). A questo proposito sono, in particolare, da segnalare: il *Digital Signature Act dello Utah*, prima legge in materia ad essere approvata; la legislazione della Florida e in specie l'*Electronic Act*, approvato nel 1996; l'ABA, *Digital Signature Guidelines*, 1996, che si pone quale schema di riferimento per i legislatori degli Stati Uniti; l'OCSE, *Guidelines for Cryptografic Policy*, 1997; l'UNCITRAL, *Planning of Future Work on Electronic Commerce: Digital Signature, Certification Authorities and Related Legal Issues*, 1997; l'EUROPEAN COMMISSION, *Ensuring Security and Trust in Electronic Communication*, 1997, COM (97) 503. I testi di tali leggi , oltre a quelli delle altre leggi emanate nel mondo per disciplinare la firma digitale o elettronica ed il commercio elettronico, sono consultabili in HYPERLINK http://www.mbc.com/ds-sum.html.

[4] La metafora è tratta da A. LISERRE, *Sul rapporto fra automazione e diritto: l'avvento del documento elettronico*, in *Riv. not.*, 1998, p. 810.

vece, accolte e recepite, conscio, da un lato, dei vantaggi che esse potranno rappresentare per la società dei prossimi anni, e, dall'altro, degli intrinseci rischi, inevitabilmente, connessi a situazioni complesse e per giunta nuove.

Sulla base di questi stimoli ed al fine di attribuire veste giuridica alle nuove fattispecie dettandone una disciplina adeguata, il legislatore ha ritenuto di dover intervenire[5] a regolare l'avvento del documento informatico[6], attraverso l'emanazione della L. 15 marzo 1997 n. 59, del D.P.R., 10 novembre 1997, n. 513, e, recentemente, del D.P.C.M. 8 febbraio 1999[7].

2. Rilevanza giuridica del documento informatico.

La validità e la rilevanza del documento informatico sono state sancite con l'emanazione dell'art. 15, comma 2, L. 59/1997[8]; il contenuto di tale norma viene, poi, ribadito dall'art. 2, D.P.R. 513[9], che, a livello regolamentare, puntualizza e precisa quanto, già, era stato disposto a livello legislativo.

L'art. 4, D.P.R. 513, prescrive che « il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta »; questo, se « munito dei requisiti previsti dal presente regolamento, ha l'efficacia probatoria prevista dall'art. 2712 c.c. » che ha riguardo alle « riproduzioni meccaniche » (art. 5, comma 2, D.P.R. 513); se, invece, « è sottoscritto con firma digitale ai sensi dell'art. 10, ha efficacia di scrittura privata ai sensi dell'art. 2702 c.c. » (art. 5, comma 1, D.P.R. 513). La firma digitale viene poi definita dall'art. 1, lett. *b*[10], e disciplinata dall'art. 10, D.P.R. 513.

---

[5] I possibili sviluppi di tale intervento sono presi in considerazione da G. Grisi, *La frontiera telematica della contrattazione a distanza*, in *Europa e diritto privato*, 1998, p. 885 s.

[6] L'espressione è di A. Liserre, *L'avvento del documento elettronico*, in *Riv. dir. civ.*, II, 1998, p. 475.

[7] Tra i primi commenti a quest'ultimo decreto (pubblicato in « *Gazzetta ufficiale* » 15 aprile 1999, n. 87): G. Finocchiaro, *La sottoscrizione on line conquista sicurezza: arriva il tassello per la conservazione degli atti*, p. 52; M. Russo - G. Cortesi, *Burocrazia: quel sogno chiamato internet*, p. 55; M. Miccoli, *Il notaio dimezzato sulla certificazione*, p. 57; tutti in *Guida al diritto*, 1º maggio 1999.

[8] Questa legge ha introdotto, all'interno dell'ordinamento una norma di portata « dirompente » che sancisce il principio della piena validità e rilevanza, a tutti gli effetti di legge, del documento informatico e del contratto stipulato in forma elettronica, disponendo, al secondo comma dell'art. 15, che « gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e 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. I criteri e le modalità di applicazione del presente comma sono stabiliti per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ».

[9] In questo articolo si precisa che « il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento ».

[10] Nel D.P.R. 513 per firma digitale s'intende « il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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 ».

Nella combinazione di queste norme (cioè artt. 4, 5 e 10 del D.P.R. 513) può essere individuato il *punto chiave* della nuova normativa, in riferimento al valore giuridico e all'efficacia probatoria del documento informatico.

Tutte le norme contenute nel D.P.R. 513/97 hanno importanza fondamentale nel legittimare e regolare l'ingresso del documento informatico nell'ordinamento giuridico; tra queste, tuttavia, le norme citate assumono un valore *speciale*. Esse, infatti, sono quelle che, grazie al complessivo impianto regolamentare in cui sono inserite, in maniera diretta riconoscono al documento informatico, inteso in senso generale, la validità e la rilevanza giuridica nell'ordinamento.

Si può, ulteriormente, notare che mediante l'art. 4, D.P.R. 513, il legislatore si riferisce ai casi in cui la legge richiede la forma scritta ma non la sottoscrizione, quindi, riconosce e legittima nel nostro ordinamento (ribadendo il disposto dell'art. 15, comma 2, L. 59/1997), la « forma informatica » come nuovo *genus* giuridico. *Genus* formato da diverse *species* di documento informatico, di cui due vengono individuate dall'art. 5, D.P.R. 513, distinguendo il tipo di conformità del documento informatico alle norme del regolamento; in quanto, il documento informatico conforme al D.P.R. 513 anche relativamente a quanto dispone l'art. 10, D.P.R. 513, configurerà la *species* disciplinata al comma 1 dell'art. 5, D.P.R. 513, cioè una « *scrittura privata informatica* », avente l'efficacia di cui all'art. 2702 c.c.; mentre, il documento informatico conforme ai requisiti del D.P.R. 513, ma non all'art. 10, D.P.R. 513, configurerà la *species* di cui al comma 2 dell'art. 5, D.P.R. 513, cioè una « *riproduzione informatica* » o una « tenuta contabile informatica », avente l'efficacia dell'art. 2712 c.c.

Nella combinazione di queste norme (artt. 4, 5 e 10 D.P.R., 513) può, anche, essere individuata la soluzione dell'annoso problema relativo alla provenienza e alla genuinità del documento elettronico, il quale aveva, fino ad ora, bloccato ogni tentativo di attribuire rilevanza giuridica ad ogni effetto al documento informatico, a causa dell'impossibilità di accertare la provenienza soggettiva (cioè l'autore del documento informatico) e l'integrità dello stesso[11].

Tale impossibilità ha rappresentato lungo questa via un ostacolo insormontabile fino all'emanazione del D.P.R. 513/97; questo, introducendo il meccanismo della firma digitale, ha in essa individuato il sistema con cui accertare la provenienza soggettiva e l'integrità del documento informatico, quindi, ha con essa introdotto la modalità in base alla quale viene determinata, con certezza, la paternità e la genuinità del documento informatico.

---

[11] Di qui l'impossibilità, fino all'emanazione del D.P.R. 513, di porre in essere documenti in forma digitale qualora la legge richiedesse a pena di nullità la forma della scrittura privata, mentre validi e rilevanti erano i documenti ottenuti con l'ausilio di un computer nei casi in cui l'ordinamento richiedeva soltanto la forma scritta. In questo senso l'opinione di R. Zagami, *Firme digitali, crittografia e validità del documento elettronico*, cit., p. 153 e di E. Giannantonio, *Il valore giurico del documento elettronico*, cit., p. 277. Considerava, invece, possibile la scrittura privata in forma elettronica B. Del Vecchio, *Riflessioni sul valore giuridico della sottoscrizione elettronica*, cit., pp. 990-992.

È stato, pertanto, il riconoscimento giuridico della firma digitale che ha consentito di porre in essere, per la prima volta nella storia del nostro ordinamento, una scrittura privata incorporata su un supporto[12] diverso da quello cartaceo, cioè su un supporto in grado di conservare una rappresentazione di natura informatica. A tal fine il legislatore ha eletto ad equipollente della sottoscrizione tradizionale il meccanismo della firma digitale operante in un sistema crittografico asimmetrico, in quanto, la « firma digitale » è in grado di perseguire, al pari della firma autografa, le finalità tipiche della sottoscrizione tradizionale[13], possedendo altresì, come l'ultima, l'indispensabile proprietà della non riutilizzabilità[14].

Il sistema della firma digitale[15] si basa, essenzialmente, sull'esistenza di

[12] I supporti fisici idonei a conservare dati digitali possono essere di vario genere (ad es. *floppy disk*, *compact disk*) e la memorizzazione dei dati digitali può avvenire con diversi metodi: cfr. G. Finocchiaro, *Documento informatico e firma digitale*, in *Contratto e Impresa*, 1998, p. 958, nota 8.

[13] La sottoscrizione può essere intesa come la scrittura autografa del nome e cognome che un soggetto appone alla fine del testo della scrittura per assumerne la paternità. Essa viene considerata come un elemento indispensabile della scrittura privata per le sue peculiari funzioni, che assumono una rilevanza decisiva affinché una scrittura privata possa essere considerata come tale: la sottoscrizione svolge, infatti, una funzione indicativa, poiché consente di identificare l'autore del documento; una funzione dichiarativa, che consiste nell'assunzione della paternità del documento da parte dell'autore dello stesso; una funzione probatoria, in quanto mezzo per provare l'autenticià del documento. Cfr., in proposito, F. Carnelutti, *Studi sulla sottoscrizione*, in *Riv. dir. comm.*, 1929, p. 513, che definisce la sottoscrizione come « l'apposizione autografa del proprio nome in calce ad un documento di cui si vuole assumere la paternità ». Si vedano inoltre P. De Lise, *Delle prove*, in *Commentario tecnico-pratico De Martino*, Roma, 1971, p. 196; L.P. Comoglio, *Tutela dei diritti*, in *Trattato Rescigno*, Torino, 1985, p. 269; V. Natoli - R. Ferrucci, *Della tutela dei diritti. Trascrizione. Prove*, in *Commentario al codice civile*, Torino, 1971, p. 338; C. Zappulli, *Il libro della tutela dei diritti, in Commentario al codice civile italiano*, Milano, 1956, p. 241; G. Cian - A. Trabucchi, *Commentario breve al codice civile*, Padova, 1984, p. 1792; S. Patti, *Della prova documentale*, in *Commentario al codice civile Scialoja-Branca*, Roma, 1996, p. 64; F. De Santis, *Della tutela dei diritti*, in *Codice civile annotato con la dottrina e la giurisprudenza* a cura di Perlingieri, VI, Napoli, 1991, p. 150. Anche la firma digitale è in grado di attuare le tre funzioni tipiche della sottoscrizione. La funzione indicativa è garantita poiché ogni firma contiene un codice numerico che identifica la chiave privata e la chiave pubblica; il codice permetterà, quindi, di reperire negli opportuni elenchi il certificato e quindi il nome associato alla firma. La funzione dichiarativa, cioè di assunzione della paternità, è assolta poiché le sue modalità operative e la specifica previsione normativa consentono di svolgere appieno tale compito. La funzione probatoria, è adempiuta in quanto dalla combinazione di firma digitale e certificato consegue certezza circa il fatto che il documento proviene dal soggetto titolare della chiave privata corrispondente alla chiave pubblica certificata. Così R. Zagami, *Firme « digitali », crittografia e validità del documento elettronico*, cit., p. 158, dove viene tuttavia rilevato che la firma digitale pur realizzando le funzioni tipiche della sottoscrizione possiede solo in parte i requisiti che dottrina e giurisprudenza attribuiscono alla sottoscrizione tradizionale.

[14] La caratteristica essenziale della non riutilizzabilità della sottoscrizione tradizionale è assicurata dalla incorporazione della stessa nel supporto materiale contenente la dichiarazione e la relativa sottoscrizione. Ogni fraudolenta utilizzazione della stessa sarà accertabile attraverso esami grafologici. La non riutilizzabilità della firma digitale è determinata da una sua precisa caratteristica tecnica, in quanto essa varia al variare del contenuto documentale, pur se apposta dallo stesso soggetto con la medesima chiave privata. Quindi ogni documento informatico ha la propria (ed unica) firma digitale.

[15] La firma digitale viene dalla dottrina definita come « un insieme di caratteri alfanumerici risultante da complesse operazioni matematiche di criptografia effettuate da un elaboratore su un documento elettronico (cioè un testo, un suono, un'im-

chiavi asimmetriche a coppia[16], una pubblica e una privata, e di enti certificatori, capaci di garantire la corrispondenza biunivoca tra la chiave pubblica e il soggetto titolare cui essa appartiene. In termini pratici, chi intende avvalersi di questo sistema dovrà, in primo luogo, dotarsi di una coppia di chiavi[17], le quali, in seguito, dovranno essere certificate da un'istituzione competente[18]. Solo a questo punto, i rapporti discendenti da un documento informatico munito di firma digitale, posto in essere dal soggetto che ha ottenuto la certificazione delle proprie chiavi, saranno giuridicamente rilevanti.

La chiave privata è l'elemento della coppia con cui si appone una firma digitale che individua, in forza di un'associazione artificiale, unicamente il soggetto titolare della stessa.

La chiave pubblica e il suo certificato, poi, consentono, rispettivamente, di stabilire, da un lato, se la firma digitale apposta o associata al documento informatico sia stata, effettivamente, apposta o associata con la chiave privata del soggetto che risulta essere il presunto sottoscrittore; dall'altro, di conoscere la reale identità del titolare della chiave privata con cui è stata apposta quella firma digitale.

---

magine e qualunque altro *file* digitale)». Così R. ZAGAMI, *Firme digitali, crittografia e validità del documento elettronico*, cit., p. 153. Essa, dunque, è il risultato di una particolare procedura informatica di validazione o di cifratura di un documento informatico ed è denominata «digitale» perché è il risultato di calcoli numerici («*digit*» in lingua inglese significa «cifra»): cfr., in questo senso, G. FINOCCHIARO, *Documento informatico firma digitale*, cit., p. 963.

La firma elettronica individua, invece, qualsiasi mezzo elettronico di identificazione. Questa, a differenza della firma digitale, non possiede la caratteristica della non riutilizzabilità, in quanto, è sempre uguale a se stessa poiché non dipendente dal contenuto del documento. Sul punto si rinvia a R. ZAGAMI, *Firme digitali, crittografia e validità del documento elettronico*, cit., p. 165. Per l'uso combinato di firma digitale e sistemi d'identificazione biometrica v. R. ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente «Atti, documenti e contratti in forma elettronica»*, cit., p. 908.

La proposta di direttiva del Parlamento europeo e del Consiglio, relativa alle regole comuni sulle firme elettroniche (98/C 325/04), disciplina il riconoscimento giuridico delle firme elettroniche e non, come la legge italiana, solo della firma digitale. La proposta, infatti, attribuisce valore legale alla firma elettronica anche se al considerando n. 6 riconosce «che tuttavia le firme digitali basate sulla crittografia a chiave pubblica costituiscono attualmente la forma più riconosciuta di firma elettronica». Ancor più forte, però, è l'esigenza di disciplinare anche altre tecniche di firma, oltre a quella digitale, così che il sistema normativo comunitario possa rispondere a qualsiasi esigenza. La firma elettronica per avere valore giuridico deve essere conforme, cumulativamente, ai requisiti indicati all'art. 2, lett. *a*, *b*, *c*, *d* della proposta di direttiva. Cfr. N. MONTANARI, *La proposta di direttiva europea sulla firma elettronica*, in *Disciplina del commercio*, 1998, p. 1001. La proposta di direttiva, quindi, legittima l'uso della firma elettronica, intesa come un vero e proprio *genus*, e della «firma elettronica avanzata», che corrisponde alla firma digitale e rappresenta solo una *species* del genere della firma elettronica.

[16] Per le modalità di funzionamento del sistema crittografico asimmetrico e per le sue caratteristiche tecniche v., in particolare, G. CIACCI, *La firma digitale*, Milano, 1999, p. 51 ss.; G. FINOCCHIARO, *Documento informatico e firma digitale*, cit., pp. 964-971.

[17] La coppia di chiavi può essere generata sia dal titolare delle chiavi, sia dal certificatore (art. 6, D.P.C.M. 8 febbraio 1999). In ogni caso, debbono essere rispettate le prescrizioni imposte dal D.P.C.M. 8 febbraio 1999 all'art. 6 (modalità di generazione delle chiavi) e all'art. 7 (generazione delle chiavi al di fuori del dispositivo di firma).

[18] Per il ruolo e l'importanza dei certificatori v., per tutti, G. FINOCCHIARO, *Documento informatico e firma digitale*, cit., pp. 971-980; R. ZAGAMI, *Firme digitali, crittografia e validità del documento informatico*, cit., p. 156.

Dall'uso combinato della chiave privata e della chiave pubblica (certificata) discende, quindi, la possibilità di accertare la provenienza soggettiva di un documento informatico munito di firma digitale e di vagliare l'integrità di quello stesso documento informatico; discende, in una parola, la garanzia dell'autenticità e della genuinità[19] del documento informatico con firma digitale.

L'apposizione della firma digitale consente infatti, in ragione delle sue caratteristiche tecniche, oltre alla verifica della provenienza soggettiva del documento, anche quella della sua integrità.

Ciò in quanto cifrare e/o apporre una firma digitale ad un documento informatico significa applicare allo stesso un algoritmo di cifratura e/o di validazione, che in base a due specifici parametri (il contenuto del documento informatico ed il codice numerico della chiave privata) rende il documento informatico illeggibile (fino alla sua decifratura), e/o metaforicamente lo « chiude » e lo rende inalterabile mediante l'apposizione o l'associazione della firma digitale.

3. Efficacia probatoria.

L'art. 5, D.P.R. 513, detta, in maniera specifica, la disciplina relativa all'efficacia probatoria del documento informatico, il quale, proprio da tale norma, viene considerato come un nuovo *genus* giuridico formato da diverse *species*, che agli occhi del legislatore sono apparse bisognose di una disciplina specifica ed adeguata alle fattispecie giuridiche cui esse danno vita.

Il documento informatico, non sottoscritto ai sensi dell'art. 10, D.P.R. 513, avrà, dunque, una forza probatoria minore rispetto a quella del documento informatico cui è apposta o associata una firma digitale. Al primo, se munito dei requisiti prescritti dal regolamento, è riconosciuta l'efficacia prevista dall'art. 2712 c.c.; mentre, al secondo è assegnata un'efficacia probatoria maggiore, cioè quella dell'art. 2702 c.c.

In base ai dati normativi richiamati sembra che la questione dell'efficacia probatoria del documento informatico munito di firma digitale sia di piana e semplice soluzione; in realtà, una specifica analisi dell'intera normativa del documento informatico, non limitata, quindi, al solo art. 5, D.P.R. 513, rivela che la « soluzione » di detta questione è, invece, alquanto « complessa »[20].

---

[19] L'autenticità e la genuinità di un documento sono caratteristiche tra loro differenti, in quanto la prima esprime la coincidenza tra la persona che ha veramente apposto la sottoscrizione con la persona indicata dalla sottoscrizione stessa come autore del documento. La genuinità esprime, invece, la coincidenza tra il testo attuale e il testo legittimo del documento; così P. Schlesinger, *La scrittura privata*, in *Jus*, 1961, p. 447.

[20] Questa soluzione è, inoltre, molto interessante, poiché collegata alla norma, da cui discendono conseguenze ed effetti giuridici, estremamente, innovativi e quasi rivoluzionari. L'art. 5, comma 1, D.P.R. 513, infatti, legittima giuridicamente, in modo specifico, la possibilità di porre in essere scritture private incorporate su supporti documentali diversi da quello cartaceo. La « legittimazione giuridica » della « scrittura privata informatica » è, ancor più « rivoluzionaria » alla luce delle proprie caratteristiche tecniche. Queste ultime, infatti, consentono che la rappresentazione del documento informatico possa assumere varie e nuove configurazioni rispetto a quanto avveniva in relazione al-

In concreto, la questione, inerente alla determinazione dell'efficacia probatoria del documento informatico munito di firma digitale, si traduce nella secca alternativa tra considerare che il regolamento consenta di qualificare *tout court* la firma digitale come « una sottoscrizione legalmente riconosciuta »; ovvero, ritenere applicabile la disciplina degli articoli 214 ss. del codice di procedura civile, quindi, considerare la firma digitale disconoscibile e verificabile in sede giudiziale.

L'art. 5 del D.P.R. 513 al comma 1 determina, attraverso il rinvio all'art. 2702 c.c., l'efficacia probatoria del documento informatico munito di firma digitale; l'art. 2702 del codice civile, circa l'efficacia della scrittura privata[21] dispone che questa « fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta ».

---

la scrittura privata tradizionale, in quanto è, ora, possibile non solo che la rappresentazione si concreti in un testo scritto ma anche, e per la prima volta, che la stessa possa assumere la forma di immagini o di suoni digitali. Il ricorso all'informatica consente, infatti, che una ripresa audiovisiva digitale o una registrazione vocale digitale, come un testo scritto digitale, costituiscano, nella medesima maniera, il contenuto del documento; poiché ognuna di queste diverse rappresentazioni, allo stesso modo, viene tradotta in *bit* e forma, così, il *file* del documento informatico il quale potrà essere, allora, firmato digitalmente quale che sia la natura dell'*input* della rappresentazione, sempre e comunque raffigurante l'insieme di *bit* costituente il contenuto del documento informatico (che potrà, indifferentemente, assumere forma scritta, sonora o audiovisiva).

La dimensione della documentazione contrattuale sarà, così, in grado di « invadere » nuovi spazi e di superare i confini tradizionalmente impostigli. Si pensi alla documentazione digitale della conclusione di un contratto attraverso la ripresa digitale dei soggetti fisici che emettono le dichiarazioni costituenti l'accordo contrattuale, la quale potrà essere firmata digitalmente dalle parti, rispettando, così, il requisito della forma scritta ai sensi dell'art. 1350 e 2702 codice civile, richiesto per i tipi contrattuali di maggior delicatezza e rilevanza giuridica. Cfr. F. DELFINI, *Il D.P.R 513/1997 e il contratto telematico*, in *Contratti*, 1998, p. 296.

[21] La disciplina della scrittura privata si limita a regolare e stabilire la rilevanza giuridica e l'efficacia probatoria della stessa, senza fornire, tuttavia, la sua definizione legale. Quest'ultima è stata elaborata dalla dottrina in via differenziale rispetto all'atto pubblico (la cui definizione è fornita dall'art. 2699 c.c.). « In senso generico, scrittura privata, è qualsiasi scritto che non sia stato compilato da un pubblico ufficiale nell'esercizio delle sue funzioni. In senso specifico, quale documento regolato dall'art. 2702 c.c., deve considerarsi qualsiasi documento scritto, che non sia redatto da un pubblico ufficiale, come tale, e che rechi la sottoscrizione di colui che abbia partecipato al negozio giuridico che la scrittura stessa deve provare »: così C. ZAPPULLI, *Il libro della tutela dei diritti*, cit., p. 240; per un'analoga definizione v. L.P. COMOGLIO, *Tutela dei diritti*, cit. p. 267. In termini più sintetici: F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1966, p. 301, secondo cui « la scrittura privata proviene, per effetto della sottoscrizione dall'autore della dichiarazione che vi è contenuta », e G. LASERRA, *La scrittura privata*, Napoli, 1959, p. 79, il quale ritiene che la scrittura privata sia « la cosa corporale su cui sono scritte parole sottoscritte da un privato nell'esercizio di una privata attività documentatrice ».

Per quanto riguarda la scrittura privata, in senso generale, si vedano, anche, B. CARPINO, voce *Scrittura privata*, in *Enc. dir.*, XLI, Milano, 1964, p. 805 ss.; S. PATTI, *Della prova documentale*, cit., p. 61; C. MANDRIOLI, *Corso di diritto processuale civile*, II, Torino, 1995, p. 191; P. SCHLESINGER, *La scrittura privata*, cit., p. 447; E. MARMOCCHI, *Scrittura privata*, in *Riv. not.*, 1987, p. 963; G. VERDE, voce *Prova documentale (dir. proc. civ.)*, in *Enc. giur. Treccani*, XXV, Roma, 1989, p. 5; U. NATOLI - R. FERRUCCI, *Della tutela dei diritti. Trascrizione. Prova*, cit., p. 336; P. DE LISE, *Delle prove*, cit., p. 194.

La scrittura privata (tradizionale) è considerata, dunque, idonea a fornire « piena prova » della provenienza della dichiarazione da chi l'ha sottoscritta se, e solo se, essa risulti essere autentica, quindi, se, e solo se, si abbia la certezza che la sottoscrizione, in calce alla scrittura privata, sia stata, effettivamente, apposta da chi appare essere l'autore della stessa.

La sottoscrizione, di per se stessa, non è, quindi, sufficiente a far conseguire l'efficacia di prova legale alla scrittura privata ai sensi dell'art. 2702 c.c.; a tal fine è, infatti, necessario che si verifichi un determinato « evento », che, statuendo l'autenticità della sottoscrizione, attribuisce alla scrittura privata la speciale forza probatoria descritta dall'art. 2702 c.c.

Ne deriva che la scrittura privata, per poter dispiegare l'efficacia di cui all'art. 2702 c.c., necessita della sussistenza di una delle cinque condizioni normative[22], a tal fine, prescritte dall'ordinamento, cioè: riconoscimento della sottoscrizione da parte di colui contro il quale la scrittura è prodotta; autenticazione della sottoscrizione *ex* art. 2703 c.c.; contumacia della parte contro cui la scrittura è stata prodotta (art. 215, n. 1, c.p.c.); mancato disconoscimento tempestivo della parte, contro cui la scrittura privata è stata prodotta (art. 215, n. 2, c.p.c); esito positivo dell'istanza di verificazione, esperita dalla parte producente la scrittura tempestivamente disconosciuta. In conclusione, il riconoscimento, espresso o tacito, l'autenticazione e la verificazione giudiziale[23] rappresentano, alternativamente, un necessario elemento costitutivo della fattispecie disciplinata dall'art. 2702 c.c.; la sussistenza di uno di questi elementi è, dunque, indispensabile affinché una scrittura privata (tradizionale) possa essere valutata come « prova legale ».

A questo punto appare necessario stabilire se anche la fattispecie costituita dalla scrittura privata informatica, al pari di quella tradizionale, necessiti della ricorrenza di uno dei descritti elementi; ovvero se essa, in ragione delle caratteristiche della firma digitale e di alcune indicazioni normative, possa *tout court* produrre efficacia di « prova legale »: al riguardo, la non apparente chiarezza dei dati normativi (si noti bene: *mancanza di chiarezza solo apparente*) consente di formulare diverse e, talora, opposte « soluzioni ». Può, infatti, essere sostenuto che la firma digitale non equivalga ad una sottoscrizione legalmente riconosciuta e che, quindi, in difetto di riconoscimento, espresso o tacito, e di autenticazione possa es-

[22] Da C. MANDRIOLI, *Corso di diritto processuale civile*, II, cit., p. 191, queste sono definite come espedienti integrativi. Egli ritiene che quando insieme con la sottoscrizione opera uno di questi espedienti integrativi il legislatore non esita ad equiparare l'efficacia probatoria della scrittura privata a quella dell'atto pubblico, limitatamente, all'aspetto della sua provenienza.

[23] In questo senso cfr., per tutti, V. DENTI, voce *Verificazione della scrittura privata*, in *Noviss. dig. it.*, XIV, Torino, 1969, p. 670, secondo cui « la verificazione della scrittura costituisce, alternativamente col riconoscimento e l'autenticazione, uno dei modi con i quali la scrittura privata acquisisce in giudizio l'efficacia probatoria prevista dall'art. 2702 codice civile. Infatti, la regola di prova legale enunciata da detta norma ha come suo presupposto l'autenticità della sottoscrizione, la quale può essere prestabilita al processo nella forma dell'autenticazione, ovvero essere acquisita nel corso del processo, attraverso il riconoscimento o la verificazione. La scrittura, poi, se autenticata, riconosciuta o verificata, forma piena prova, fino a querela di falso, della provenienza della dichiarazione da chi l'ha sottoscritta ».

sere disconosciuta e fatta, successivamente, oggetto di verificazione *ex* art. 216 c.p.c.[24].

In questa sede si ritiene, invece, che la soluzione più aderente, da un lato, al contenuto della disciplina del documento informatico e, dall'altro, alla logica del sistema della firma digitale, si concreti, necessariamente, nel constatare che « il documento informatico sottoscritto con firma digitale ai sensi dell'art. 10, D.P.R. 513 » fa piena prova fino a querela di falso prescindendo dall'intervento di una delle condizioni normative richieste dall'art. 2702 c.c. (che risultano, allora, necessarie, ai fini dell'acquisizione del valore di prova legale, solo in relazione alla scrittura privata tradizionale).

4. (Segue) Scrittura privata informatica come prova legale.

La soluzione, al momento soltanto enunciata, trova il suo fondamento e la sua giustificazione in una serie di argomentazioni che, da un lato, sono legate alle caratteristiche intrinseche del sistema della firma digitale, da altro lato, alle recenti scelte normative dettate da queste caratteristiche.

In questo contesto va, in primo luogo, osservato che il rinvio effettuato dall'art. 5, comma 1, D.P.R. 513, all'art. 2702 c.c. (« il documento informatico ha efficacia di scrittura privata ai sensi dell'art. 2702 c.c. »), in ragione del modo in cui è stato formulato, sembra richiamare soltanto il tipo di efficacia probatoria prevista da tale norma, non, quindi, l'intera fattispecie astratta dalla stessa norma regolata[25].

---

[24] A favore di questa soluzione F. De Santis, *La disciplina del documento informatico. Il commento*, in *Corriere giuridico*, 1998, p. 392 s., che ritiene « praticabile, su un piano strettamente tecnico, il procedimento di verificazione in quanto inteso ad accertare (attraverso il rispetto dei criteri di formazione previsti dal regolamento) la provenienza del documento informatico, dato che il disconoscimento ha ad oggetto l'autenticità della firma digitale stessa »; F. Ferrari, *La nuova disciplina del documento informatico*, in *Riv. dir. proc.*, 1999, pp. 144-148, la quale sottolinea il fatto che « il procedimento di certificazione precedente al rilascio della chiave pubblica fornisce una certezza solo in ordine all'identificazione del soggetto che ha richiesto la chiave medesima, ma non consente di escludere il rischio che, successivamente, al rilascio, qualcun altro utilizzi illegittimamente la chiave rilasciata al titolare. L'esistenza di questo rischio impone di considerare imprescindibile il riconoscimento del documento informatico da parte del soggetto contro il quale lo stesso è prodotto ».

Anche L. Albertini, *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ.*, II, 1998 p. 288 s., giunge ad analoghe conclusioni affermando, in particolare, che « stante la presenza nel nostro ordinamento di due precisi elementi della fattispecie costitutiva del vincolo probatorio legale cioè l'autenticazione, da un lato, e il riconoscimento, espresso o tacito *ex* art. 215 c.p.c., dall'altro, deve ritenersi — in assenza di indici contrari — non certo che quest'ultimo sia stato escluso, bensì, piuttosto e al contrario, che nulla osta al loro permanere: è infatti più ragionevole ritenere che l'eventuale esclusione di una norma fondamentale come gli artt. 214 e 215 c.p.c. dovesse essere esplicita ». Oppure si può, al contrario, ritenere che la natura e le caratteristiche della firma digitale rendono tale esclusione talmente palese che non risulta, quindi, necessaria una precisa indicazione normativa al riguardo.

Si cercherà, nel prosieguo, di mettere in luce che la provenienza del documento informatico munito di firma digitale non deve essere accertata attraverso la verificazione giudiziale della stessa *ex* art. 216 c.p.c. e che il rischio dell'uso abusivo della chiave privata non può essere ostacolato ed evitato dalla possibilità di disconoscere una firma digitale.

[25] In questo senso A. Graziosi, *Premesse ad una teoria probatoria del docu-*

È, poi, la differente modalità con cui si stabilisce la paternità di un documento, rispettivamente, attraverso il meccanismo della firma digitale, da un lato, e quello della sottoscrizione tradizionale, dall'altro, a rendere inconcepibile la possibilità di disconoscere una firma digitale. Infatti, l'esclusivo collegamento, di natura soggettiva, intercorrente tra firma autografa e proprio autore, caratteristico della sottoscrizione tradizionale, idoneo ad individuare ciascun soggetto attraverso il proprio ed esclusivo stile grafico, si trasforma in un'associazione artificiale ed oggettiva tra firma digitale e titolare della chiave privata con cui la prima è stata apposta. Questo tipo di associazione non è in grado, a differenza del collegamento di diversa natura proprio della sottoscrizione tradizionale, di individuare l'effettivo autore di una determinata firma digitale facendo leva sulla personalità grafica del segno, ma è in grado di stabilire, soltanto, che una determinata firma digitale proviene da una determinata chiave privata, attribuita, in via esclusiva attraverso la certificazione, ad un solo soggetto.

Dal differente rapporto che intercorre tra firma autografa, da una parte, firma digitale, dall'altra, e soggetto cui sono riferite, discende che, da un punto di vista logico, la natura della sottoscrizione tradizionale permette al soggetto, contro cui sia prodotta una scrittura privata (tradizionale), di poter affermare o negare che quella sottoscrizione provenga, effettivamente, da lui, in ragione della possibile alternativa tra autenticità e falsità del segno grafico, accertabile, di volta in volta, solo in seguito a complessi esami grafologici. Il collegamento, prettamente oggettivo, tra titolare della chiave con cui la firma digitale viene apposta e medesima firma digitale, invece, non concede, assolutamente, allo stesso tale possibilità.

La firma digitale infatti, in caso di verifica con esito positivo[26], è collegata, con certezza matematica, unicamente al titolare della chiave privata utilizzata per la sua apposizione in forza del nesso artificiale tra chiavi crittografiche e loro titolare[27]. Non permane spazio alcuno per la sussistenza,

mento informatico, in *Riv. trim. dir. proc. civ.*, 1998, p. 515, secondo il quale se il legislatore avesse voluto richiamare l'intera disciplina dell'art. 2702 c.c. avrebbe, di certo, utilizzato formule diverse da quella dell'art. 5, comma 1, D.P.R. 513, come ad es.: « nei casi previsti dall'art. 2702 c.c., il documento informatico sottoscritto con firma digitale fa piena prova fino a querela di falso » ovvero « il documento informatico fa piena prova fino a querela di falso quando ricorre una delle condizioni di cui all'art. 2702 c.c. ... ». Così, ma in maniera più sintetica, anche G. Finocchiaro, *Documento informatico e firma digitale*, cit., p. 984.

[26] La verifica della firma digitale corrisponde al controllo effettuabile sulla stessa utilizzando il sistema di validazione (art. 1, lett. *c*, D.P.R. 513), previa consultazione e reperimento del certificato della chiave pubblica corrispondente a quella privata con cui la firma digitale è stata apposta. Verifica, dunque, che non ha niente a che vedere con i controlli effettuati dall'autorità giudiziaria su una firma autografa in sede di verificazione *ex* art. 216 c.p.c.

[27] Così, A. Gentili, *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ.*, II, 1998, p. 173, e M. Orlandi, *L'imputazione dei testi informatici*, in *Riv. not.*, 1998, pp. 889, 871, 872, 873. Il primo, infatti, afferma che « il riferimento della firma digitale al titolare è intrinseco al sistema ed il disconoscimento può avere solo il senso di affermare non l'inautenticità ma l'abuso, e quindi di sfidare chi invoca la scrittura a dare la prova negativa dell'illecito utilizzo »; il disconoscimento, dunque, perde la sua caratteristica principale e fondante cioè la negazione della riferibilità della firma all'apparente sottoscrittore attraverso la denuncia della contraffazione della firma autografa. Per il secondo « la firma digitale è intrinsecamente incapace di restituire la prova della paternità materiale, giacché rappresenta non l'autore della digitazione bensì il titolare della digitazione »; quindi « che l'autore materiale della firma (il digitatore della chiave) sia Tizio o Caio nulla più rilevereb-

anche da un punto di vista logico, del fatto denunciato con il disconoscimento, cioè della *mancanza del nesso di riferibilità del segno grafico (non digitale)* a chi appare il presunto sottoscrittore, che avendo natura soggettiva deve ogni volta, se contestato, essere verificato (ai sensi dell'art. 216 c.p.c.) data la possibilità di una sua contraffazione. Mentre, il nesso oggettivo, se la firma digitale è riconosciuta valida applicando alla stessa la chiave pubblica corrispondente, non potrà formare oggetto di tale contestazione e, conseguentemente, non potrà essere sottoposto a questo nuovo esame poiché detto nesso non è idoneo, da un punto di vista logico, a dar vita all'alternativa tra autenticità e falsità del *segno digitale*. Ciò in considerazione della quasi assoluta impossibilità di una sua contraffazione[28], risultando il segno digitale soltanto idoneo a configurare l'ipotesi di utilizzo lecito od illecito della chiave privata con cui apporre una firma digitale, che, in entrambi i casi, corrisponderà, comunque, ad un *segno digitale* di per se stesso (inteso, cioè, esclusivamente da un punto di vista materiale) valido ed autentico (sempre se, si ribadisce, la firma digitale sia ritenuta autentica dal sistema di validazione del destinatario del documento informatico).

Tale costruzione logica viene poi confortata da precise indicazioni normative, che, dunque, avvalorano le conclusioni raggiunte mettendo in luce la diversa natura della firma digitale e della sottoscrizione tradizionale tramite l'analisi comparata di queste entità fenomeniche[29].

A tal fine è necessario richiamare il contenuto di alcune norme a cui, finora, non è stata attribuita la dovuta importanza in materia di efficacia probatoria della scrittura privata informatica, cioè l'art. 1, lett. *f*; l'art. 1, lett. *b*; l'art. 1, lett. *c*, D.P.R. 513.

5. (Segue) « Presunzione di riferibilità »; « nuova verificazione ».

Le norme sopracitate, dettate all'interno dell'art. 1, D.P.R. 513, (che già nella rubrica precisa il suo riferimento alle « definizioni »[30]), costitui-

---

be, poiché l'oggettiva apposizione del codice digitale potrà essere in sé sufficiente per imputare la scrittura al titolare della chiave » (pp. 873, 871).

[28] La conoscenza della chiave pubblica non dà alcuna indicazione per la « ricostruzione » della chiave privata, quindi, una sua ipotetica contraffazione è assai improbabile se non impossibile; anche perché il D.P.C.M. 8 febbraio 1999 prevede che le caratteristiche tecniche delle chiavi siano tali da assicurare un alto livello della loro « robustezza » (art. 4, comma 6, artt. 5, 6, 7, 8, e 10 del D.P.C.M.).

La sicurezza del sistema crittografico non è, però, dimostrabile matematicamente ma è di tipo computazionale, è basata, cioè, sulla considerazione della quantità di lavoro necessario per forzare il sistema, utilizzando l'attuale capacità di calcolo degli elaboratori elettronici: così G. Finocchiaro, *Documento informatico e firma digitale*, cit., p. 966.

[29] Il parallelismo che il legislatore sembra voler introdurre fra scrittura privata tradizionale e scrittura privata informatica subisce, quindi, « dalla natura delle cose alterazioni che fanno dubitare se veramente possa all'una ed all'altra essere applicata la stessa disciplina »: così A. Gentili, *Documento informatico e tutela dell'affidamento*, cit., p. 171.

[30] In merito al ruolo assegnato alle definizioni cfr., in particolare, U. Scarpelli, *La definizione nel diritto*, in *Jus*, 1959, p. 496 ss.; A. Belvedere, *Il problema delle definizioni*, in *Riv. dir. civ.*, I, 1978, p. 268 ss.; G. Tarello, *L'interpretazione della legge*, in *Tratatto di diritto civile e commerciale* diretto da Cicu e Messineo e con-

scono disposizioni legislative di notevole rilevanza circa l'efficacia probatoria della firma digitale e, di conseguenza, della scrittura privata informatica.

Fondamentale, al fine di quanto si dirà in seguito, è l'art. 1, lett. *f*, D.P.R. 513, il quale dispone che « per chiave pubblica s'intende l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si *verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche...* ». In questa norma viene specificata la funzione precipua che la chiave pubblica assolve: questa, se utilizzata unitamente al sistema di validazione (art. 1, lett. *c*, D.P.R. 513) serve per accertare la validità della firma digitale e, contemporaneamente, per individuare chi ha apposto quella firma digitale.

Il perseguimento di quest'ultima finalità, cioè l'individuazione del soggetto cui riferire la firma digitale, è reso possibile dal legislatore stesso che, in questa norma, indica, in maniera puntuale, il soggetto cui riferire la firma digitale verificata e valida.

Nell'art. 1, lett. *f*, D.P.R. 513, il soggetto che appone la firma digitale verificata con una determinata chiave pubblica non è, infatti, indicato dal legislatore in maniera generica ma, in forza di una sua precisa disposizione, appare essere un soggetto fortemente determinato, cioè il « TITOLARE delle chiavi asimmetriche »[31] utilizzate, rispettivamente, per apporre e per verificare quella firma digitale.

---

tinuato da Mengoni, I, 2, Milano, 1980, p. 153 ss.; R. QUADRI, *Dell'applicazione della legge in generale*, in *Commentario al codice civile Scialoja e Branca, Disposizioni sulla legge in generale, art. 10-15*, Bologna-Roma, 1974, p. 267; A. GIULIANI, *Le disposizioni sulla legge in generale: gli artt. da 1 a 15*, in *Trattato di diritto privato* diretto da Rescigno, I, *Premesse preliminari*, Torino, 1982, p. 222; R. GUASTINI, *Teoria e dogmatica delle fonti*, in *Trattato di diritto civile e commerciale* diretto da Cicu e Messineo e continuato da Mengoni, I, 1, Milano, 1998, p. 2 ss.

[31] « S'intende per titolare di una coppia di chiavi asimmetriche, il soggetto cui è attribuita la firma digitale generata con la chiave privata della coppia » (art. 1, lett. *a*, D.P.C.M. 8 febbraio 1999). Anche le regole tecniche dove, appunto, viene delineata, ulteriormente, la figura del titolare delle chiavi crittografiche, evidenziano l'inevitabile riferibilità della firma digitale al titolare della chiave privata utilizzata per apporre quella firma (« ... il soggetto cui è attribuita la firma digitale generata con la chiave privata della coppia »).

Dal combinato disposto dell'art. 1, lett. *f*, D.P.R. 513 e dell'art. 1, lett. *a*, D.P.C.M. 8 febbraio 1999 discende la regola in forza della quale si raggiunge, presuntivamente, la certezza relativa alla paternità della firma digitale. Le norme in questione, tra loro complementari, creano insieme la modalità in base alla quale si attribuisce la firma digitale al suo autore, stabilendo, letteralmente, una sorta di circolare riferibilità della firma digitale al titolare delle chiavi crittografiche: l'art. 1, lett. *f*, D.P.R. 513, infatti, attribuisce, in un senso, la firma digitale verificata positivamente con la chiave pubblica al titolare di quest'ultima; l'art. 1, lett. *a*, D.P.C.M. 8 febbraio 1999, in senso inverso, attribuisce la firma digitale al soggetto titolare della chiave privata con cui la firma digitale è stata generata. La firma digitale, quindi, in un senso o nell'altro, si riferisce, comunque, al titolare delle chiavi crittografiche usate, rispettivamente, per apporre e per verificare quella firma digitale (essa sembra, così, stabilire con il suo autore un inscindibile legame di natura circolare, in quanto, in un senso, essa individua la chiave privata usata per la sua apposizione, in un altro senso, quella pubblica usata per la verifica; di conseguenza, in entrambi i sensi individua, sempre, lo stesso soggetto, cioè il titolare delle chiavi crittografiche *ex* art. 1, lett. *f*, D.P.R. 513, e *ex* art. 1, lett. *a*, D.P.C.M. 8 febbraio 1999).

Tale descrizione non fa altro che ribadire il funzionamento del sistema crittografico asimmetrico, ma dato che lo fa a livello normativo avrà valore precettivo e non mero valore rappresentativo. Si è in grado, così, di generare certezza circa la paternità della firma digitale, in caso della sua verifi-

È, infatti, letteralmente disposto che la verifica della firma digitale, effettuata con l'ausilio del sistema di validazione e di una chiave pubblica, qualora abbia esito positivo, individua il TITOLARE della coppia di chiavi crittografiche, con il cui elemento privato è stata apposta quella firma digitale, in seguito, verificata con il corrispondente elemento pubblico, e non genericamente la chiave privata con cui quella firma digitale è stata apposta e, di conseguenza, genericamente ogni suo ipotetico effettivo utilizzatore.

La disposizione in questione si concreta, dunque, in una vera e propria presunzione di riferibilità della firma digitale al TITOLARE della chiave privata con cui quella firma digitale è stata apposta e verificata ai sensi dell'art. 1 lett. *c* ed *f*[32], D.P.R. 513. In forza di tale presunzione, viene determinata *a priori* la provenienza soggettiva di un documento informatico con firma digitale, la cui paternità è, necessariamente, attribuita *ex lege* al titolare della chiave privata con cui la firma digitale è stata apposta.

La presunzione di riferibilità prescritta dall'art. 1, lett. *f*, D.P.R. 513, si adegua, pienamente, alla logica del sistema crittografico asimmetrico[33] e

---

ca positiva, come se si fosse verificata una delle condizioni normative richieste dall'art. 2702 c.c. in relazione alla sottoscrizione tradizionale (la cui ricorrenza, invece, non è necessaria per la firma digitale in forza, appunto, della sua presunzione legislativa di riferibilità, che da sola esplica la funzione tipica di dette condizioni normative).

[32] Anche altri dati normativi, in maniera indiretta, depongono in favore della sussistenza di tale presunzione di riferibilità. Essi, uniti al disposto dell'art. 1, lett. *f*, D.P.R. 513, dal quale, direttamente, discende la presunzione, rafforzano il fondamento normativo della sua esistenza e, quindi, anche la sua portata precettiva. Tra questi vanno, in particolare, richiamati l'art. 1, lett. *b*, D.P.R. 513, il quale dispone che *l'uso della chiave pubblica consente di verificare la provenienza* di un documento informatico con firma digitale. La verifica in questione lascia spazio solo a due alternative: la firma digitale è stata apposta con la chiave privata corrispondente a quella pubblica usata per effettuare la verifica; ovvero, la firma digitale non risulta essere stata apposta con la chiave privata corrispondente. Nel secondo caso non si raggiunge alcuna certezza sulla provenienza del documento informatico, se non quella relativa al fatto che la firma digitale non proviene da chi appare essere l'autore del documento; nel primo caso invece, la certezza sulla provenienza del documento informatico viene raggiunta. E per certezza sulla provenienza si può, soltanto, intendere che la firma digitale proviene da un solo soggetto, cioè il titolare delle chiavi crittografiche.

L'art. 10, comma 3, D.P.R. 513, poi, prescrive che la firma digitale « deve *riferirsi in maniera univoca ad un solo soggetto* »; ebbene pur non specificando, in modo puntuale, chi sia questo soggetto, esso, alla luce del funzionamento del sistema crittografico asimmetrico, non potrà che essere il titolare delle chiavi crittografiche usate, rispettivamente, per apporre e verificare la firma digitale. A tale soggetto soltanto, come dispone la norma in questione, potrà, dunque, essere riferita, « in maniera univoca », la firma digitale. L'univoca riferibilità della firma digitale ad un solo soggetto, cioè il titolare delle chiavi crittografiche, viene, altresì, ribadita dall'art. 4, D.P.C.M. 8 febbraio 1999, secondo cui « una coppia di chiavi può essere attribuita ad un solo titolare » che, di conseguenza, risulterà essere l'unico soggetto individuabile in seguito alla verifica della firma digitale apposta con la sua chiave privata e, quindi, l'unico soggetto cui attribuire la paternità di quella firma digitale.

[33] Il legislatore è consapevole che la corrispondenza, presunta *ex lege*, tra titolare delle chiavi crittografiche e reale utilizzatore di quella privata, potrà, in alcuni casi, non coincidere alla realtà delle cose; quindi, al fine di aumentare la probabilità che il reale utilizzatore della chiave privata corrisponda a quello individuato *ex lege*, cioè il titolare delle chiavi crittografiche, viene nell'allegato tecnico disposto che « prima di procedere alla generazione della firma, il dispositivo deve procedere all'identificazione del titolare » (art. 10, comma 4, D.P.C.M. 8 febbraio 1999). Tale « regola tecnica », persegue, principalmente, lo scopo di garantire, il più possibile, la

si concreta in un elemento idoneo, da solo, a far acquisire alla firma digitale il valore probatorio della sottoscrizione legalmente riconosciuta, facendo, così, venir meno la necessità dell'autenticazione ai sensi dell'art. 2703 c.c. (ma non dell'art. 16, D.P.R. 513[34]) e del riconoscimento,

corrispondenza tra titolare delle chiavi crittografiche (cioè presunto utilizzatore della chiave privata) e reale utilizzatore della chiave privata.

L'identificazione del titolare ai sensi dell'art. 10, comma 4, D.P.C.M. 8 febbraio 1999 sarà, probabilmente, effettuata tramite le c.d. chiavi biometriche, definite dall'art. 1, lett. *g*, D.P.R. 513 (R. ZAGAMI, *Firme digitali, crittografia e validità del documento informatico*, cit., p. 166, ipotizzava, già, un uso combinato di firme digitali e codici d'identificazione biometrici). Sulla funzione delle chiavi biometriche v., in particolare, E. MACCARONE, *Chiavi biometriche*, relazione al convegno « Documento informatico, firma digitale e commercio elettronico », Università di Camerino 29-30 ottobre 1999, spec. p 3-7, in Atti del convegno (in corso di stampa), e in http//www.unicam.it/ssdici/convegno_ott.html.

[34] La specifica previsione normativa dell'autenticazione della firma digitale (art. 16, D.P.R. 513) non deve essere considerata come un ostacolo per l'attribuzione del valore di prova legale alla firma digitale, pur se non riconosciuta e, appunto, non autenticata; in specie, non deve essere considerata come un elemento contrastante con l'idea che la firma digitale ha efficacia di scrittura privata legalmente riconosciuta, pur se non autenticata da notaio o altro pubblico ufficiale *ex* art. 2703 c.c. Il legislatore, infatti, ha sì individuato giuridicamente una specifica ipotesi in cui la firma digitale acquisisce valore di sottoscrizione legalmente riconosciuta ai sensi dell'art. 2703 c.c. Esso, però, ha anche stabilito, altrettanto precisamente, il tipo di controllo che l'autorità fidefacente deve effettuare. Questa, infatti, non si deve limitare, unicamente, ad identificare il soggetto che sottoscrive la scrittura privata, che in forza di tale controllo, diviene autenticata, ma deve, a tal fine, *ex* art. 16, D.P.R. 513, effettuare ulteriori accertamenti giuridicamente non previsti in caso di sottoscrizione tradizionale, in quanto « l'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto corrisponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, numero 1, della legge 16 febbraio 1913, n. 89 ». La firma digitale autenticata è, dunque, in grado di attribuire pubblica fede ad elementi rispetto ai quali la sottoscrizione tradizionale autenticata non fornisce, invece, la stessa garanzia. Necessaria conseguenza è, allora, il fatto che l'autentica della firma digitale rispetto a quella della sottoscrizione tradizionale rappresenta qualcosa in più e, soprattutto, qualcosa di diverso, cioè un procedimento fidefacente più penetrante (v., anche R. ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente « Atti, documenti e contratti in forma elettronica »*, cit., p. 912, nota 34). Ciò giustifica la specifica previsione legislativa di cui all'art. 16, D.P.R. 513, la cui *ratio* si individua nella necessità di creare un procedimento autenticativo proprio della firma digitale, quindi conforme alle sue caratteristiche e diverso da quello tipico della sottoscrizione tradizionale. Esso, dunque, in ultima analisi, appare non suscettibile di essere considerato come unico strumento (in alternativa al riconoscimento e alla verificazione giudiziale) capace di attribuire valore di prova legale alla firma digitale, poiché essa, già, possiede tale valore. E l'ordinamento lo riconosce, ulteriormente, anche attraverso il fatto che l'autentica *ex* art. 16, D.P.R. 513, non attribuisce alla firma digitale valore di prova legale ma gli attribuisce, invece, una forza probatoria più ampia rispetto a quella di cui all'art. 2703 c.c. (in questo senso, anche, A. GENTILI, *Documento informatico e tutela dell'affidamento*, cit., p. 172 s.). L'art. 16, D.P.R. 513, allora, si armonizza, pienamente, con il sistema della firma digitale. Questa, infatti, come spiegato, individua, già, con una sorta di evidenza pubblica il soggetto da cui proviene, *rectius* da cui si presume, anche legalmente, provenire, senza necessità di una sua autenticazione. La sua autenticazione *ex* art. 16, D.P.R. 513, va quindi oltre e garantisce non solo la provenienza soggettiva del documento con firma digitale, assicurata già in ampia misura dal sistema. Essa, in virtù di controlli più incisivi, garantisce, anche e soprattutto, circa il fatto che la chiave privata utilizzata per apporre la firma digitale (autenticata) era, ancora, valida al momento della « firma »; che quanto contenu-

espresso o tacito (ai sensi degli artt. 214, 215 c.p.c.). Così, in relazione alla firma digitale, a differenza di quanto accade circa la fattispecie della sottoscrizione tradizionale, il legislatore predispone una condizione normativa che *a priori* attribuisce alla firma digitale l'efficacia probatoria di cui agli artt. 2702 e 2703 c.c., senza che intervengano *a posteriori* le ulteriori condizioni normative, che risultano, a tal fine, necessarie, soltanto, nei confronti della firma autografa che, a differenza della firma digitale, non è riferibile, presuntivamente, a chi appare essere il suo autore, data la differente natura del rapporto che intercorre fra esse e i loro presunti autori.

L'efficacia probatoria riconosciuta alla firma digitale attraverso la presunzione di riferibilità dell'art. 1 lett. *f*, D.P.R. 513, non lascia spazio alcuno, anche e soprattutto da un punto di vista giuridico, al disconoscimento della firma digitale, in quanto, in seguito a verifica positiva (*ex* art. 1, lett. *c*, D.P.R. 513), essa acquisisce, immediatamente, forza probatoria pari a quella di una sottoscrizione legalmente riconosciuta, che, secondo i princìpi del nostro ordinamento, non può essere contestata attraverso l'istituto processuale del disconoscimento ma, soltanto, tramite querela di falso.

Tale affermazione può essere, altresì, corroborata da ulteriori indicazioni legislative. L'art. 1, lett. *c*, D.P.R. 513, infatti, dispone che « per sistema di validazione s'intende il sistema informatico e crittografico in grado di generare ed apporre la firma digitale e di *verificarne* la validità »; il termine « *verifica* » viene poi utilizzato anche in altre norme, cioè negli artt. 1, lett. *b*; 1, lett. *f*, D.P.R. 513; negli artt. 4, comma 4, lett. *a*; 10, commi 1 e 6, D.P.C.M. 8 febbraio 1999.

L'uso così frequente di questa specifica terminologia e soprattutto della locuzione dell'art. 1, lett. *c*, D.P.R. 513 (« *verificarne la validità* ») potrebbe evocare, entro certi limiti, l'istituto regolato dall'art. 216 c.p.c., cioè l'istanza di verificazione. Questa, è richiesta dalla parte che intende valersi della scrittura disconosciuta, proponendo i mezzi di prova che ritiene utili e indicando le scritture che possono servire da comparazione.

---

to nel documento, risponde alla volontà della parte che lo ha sottoscritto (ciò tramite la ricognizione del contenuto della dichiarazione estrinsecata nel documento e della rispondenza del dichiarato al voluto, così da escludere i vizi del volere eliminabili attraverso tale accertamento, come l'errore; non la violenza che potrebbe essere precedente e non contestuale all'esternazione della dichiarazione); che il contenuto del documento sia lecito.

Di conseguenza, con la querela di falso esperibile contro il documento informatico autenticato si potrà, esclusivamente, denunciare il c.d. falso ideologico, cioè la mendacità dell'attestazione del pubblico ufficiale o delle dichiarazioni del privato ma non l'illecito utilizzo della chiave privata utilizzata per apporre la firma digitale autenticata (per le possibili ipotesi di infedele autentica notarile si rinvia a R. Zagami, *op. ult. cit.*, p. 923, nota 78). L'oggetto della querela di falso, quindi, avrà in questo caso una « latitudine sostanziale » ridotta rispetto a quello della querela esperita contro un documento informatico non autenticato. Contro quest'ultimo, infatti, tramite querela di falso può essere denunciato, anche, l'uso abusivo della chiave privata da parte di terzi; la cui ricorrenza è, invece, necessariamente esclusa in caso di autenticazione di firma digitale *ex* art. 16, D.P.R. 513. In questo senso cfr., anche, A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, cit., p. 517 s.; G. Finocchiaro, *Documento informatico e firma digitale*, cit., p. 986. In merito alla firma digitale autenticata, in senso generale, si veda, anche, G. Petrelli, *Documento informatico, contratto in forma elettronica e atto notarile*, in *Notariato*, 1997, pp. 581-583.

Dalle risultanze di detta istanza deriva, in seguito alla valutazione dell'autorità giudiziaria, l'attribuzione o no dell'efficacia probatoria di scrittura privata legalmente riconosciuta, ai sensi degli artt. 2702 e 2703 c.c., al documento verificato .

Efficacia che verrà riconosciuta se le prove addotte saranno in grado di ingenerare nel giudice la « certezza » che la scrittura proviene dal soggetto che appariva essere il « presunto sottoscrittore » e che, dopo la pronuncia del giudice in merito a detta questione, non è più da ritenere come « presunto sottoscrittore » ma deve, da questo momento, essere considerato, invece, come « l'effettivo sottoscrittore » della scrittura privata.

Tutto questo perché si è raggiunta la certezza sulla « paternità » della scrittura privata; viene, quindi, garantito, in ragione delle risultanze della verificazione processuale, che quella scrittura proviene effettivamente dal soggetto « contemplato », cioè da colui che ha apposto manualmente in calce al documento il proprio nome e cognome.

Ebbene, la finalità sostanziale dell'istanza di verificazione (art. 216 c.p.c.), cioè il raggiungimento della « certezza » relativa alla « paternità » e alla « provenienza soggettiva » di una scrittura privata, è la stessa di quella realizzata dalla « verifica di validità » della firma digitale, effettuata con l'ausilio del « sistema di validazione » (art. 1, lett. *c*, D.P.R. 513). Dall'uso del quale discende che la sicurezza e la certezza sulla provenienza soggettiva del documento con firma digitale si raggiunge anche senza il bisogno e la necessità di riconoscimento o di verificazione giudiziale.

Tale « certezza » è, infatti, logicamente, intrinseca al sistema della firma digitale e viene, semplicemente, garantita, da un lato, dal fatto che il certificato contenente la chiave pubblica non sia revocato, sospeso o scaduto; dall'altro, dal fatto che la firma digitale verificata con l'ausilio del sistema di validazione e della predetta chiave pubblica, sia riconosciuta come valida. « Certezza » che, poi, oltre ad essere intrinsecamente connessa al sistema crittografico asimmetrico, è, anche, esplicitamente sancita dal legislatore attraverso la presunzione di riferibilità della firma digitale al titolare delle chiavi crittografiche usate, rispettivamente, per l'apposizione e le verifica della firma digitale. Ciò consente, pertanto, di perseguire, *prima e fuori* della fase giudiziale, quanto viene raggiunto, in sede processuale, dall'istanza di verificazione. Istanza che, visto che il suo scopo viene, già, realizzato al di fuori della sede giudiziale, appare, sicuramente, superflua e, dunque, non adatta ad accertare o caducare l'efficacia probatoria del documento informatico munito di firma digitale. Anche e soprattutto perché tale efficacia è stabilita presuntivamente *ex lege* ed è tale da non poter essere contestata tramite semplice disconoscimento della scrittura e, di conseguenza, non è suscettibile dell'eventuale e successivo accertamento che costituisce l'oggetto della verificazione *ex* art. 216 c.p.c. Verificazione che, dunque, sembrerebbe « *trasposta* » al di fuori del processo[35].

[35] La scrittura privata informatica è, al pari di quella tradizionale, una prova precostituita poiché si forma fuori e prima del processo, nel quale entra attraverso un semplice atto di esibizione o di produzione. I documenti sono, già per se stessi, dotati dell'attitudine a produrre efficacia probatoria, sicché a produzione avvenuta, al giudice non rimane da svolgere altra attività, rispetto ad essi, se non quella del loro apprezzamento, o valutazione, ossia un'attività che già concerne la fase di decisione e non anche quella di istruzione (cfr. C. MANDRIOLI, *Corso di diritto processuale civile*, II, cit., p. 141 s.). Nel caso, però, di scrittura privata informatica la novità e

Ciò in quanto il soggetto privato è in grado di poter determinare, da solo, con il semplice ausilio del sistema di validazione e con la consultazione *on line* dell'elenco dei certificati, quanto viene determinato dal giudice in sede giudiziale in seguito ad istanza di verificazione: cioè, che la firma digitale è autentica poiché è apposta con una chiave privata, corrispondente ad una chiave pubblica certificata (ancora valida); firma digitale che dalla stesso ordinamento è, poi, riferita, univocamente, al titolare delle chiavi crittografiche (*ex* art. 1, lett. *f*, D.P.R. 513).

Detta « trasposizione » sembra essere, dunque, evocata sia da ragioni di ordine sostanziale che da ragioni di ordine letterale. Da un lato, per il motivo che entrambe le forme di verificazione perseguono lo stesso scopo sostanziale; dall'altro, per il fatto che il legislatore ha utilizzato lo stesso termine « verificare », forse, consapevole della sua capacità « evocatoria », per richiamare, quanto meno, i soli effetti sostanziali, e non la disciplina formale, della verificazione processuale.

Pertanto, per « trasposizione » della verificazione dalla sede processuale a quella privata s'intende che l'uso corretto del sistema di validazione da parte del privato (*ex* art. 1, lett. *c* e *ex* art. 1, lett. *f* D.P.R. 513) realizza, nella stessa misura, l'effetto sostanziale che consegue alle risultanze dell'istanza di verificazione *ex* art. 216 c.p.c., e quindi che la verificazione di cui all'art. 1, lett. *c*, D.P.R. 513 fornisce la stessa garanzia, circa la « provenienza soggettiva » di una scrittura privata tradizionale.

---

la peculiarità del mezzo di prova che essa costituisce, renderà necessario un « controllo » della stessa da parte del giudice istruttore, al fine di accertare la validità della firma digitale della scrittura privata informatica, tramite l'ausilio di un computer e di un apposito sistema di validazione. Il controllo in questione si risolverà in un'operazione veloce e semplice, che, nella maggior parte dei casi, non richiederà l'intervento di un consulente tecnico (sul punto v. A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, cit., p. 493 s.) e che non potrà considerarsi come un procedimento di assunzione di prova costituenda, poiché la prova rappresentata da una scrittura privata informatica è, completamente, precostituita al processo. Tale « controllo » non potrà, nemmeno, essere considerato come un'istanza di verificazione *ex* art. 216 c.p.c., in quanto esso deve essere effettuato ogni volta che un documento informatico con firma digitale venga prodotto in giudizio e non, soltanto, nel caso in cui la parte contro cui tale documento sia prodotto lo disconosca. Questo « controllo » dovrà, dunque, essere « necessario » e non, come la verificazione *ex* art. 216 c.p.c., soltanto « eventuale ». È, infatti, necessario che l'autorità giurisdizionale accerti, direttamente, quanto la parte che produce il documento informatico dichiara, cioè che la firma digitale è risultata valida in seguito a verifica della stessa *ex* art. 1, lett. *c*, D.P.R. 513. Ciò per il semplice motivo che tale forma di « controllo » risulta essere rapida ed agevole. L'ingresso in giudizio di una scrittura privata informatica avverà, dunque, nello stesso modo in cui avviene quello delle altre prove precostituite, ma, a differenza delle ultime, sarà, in un certo senso, condizionato dalle risultanze del « necessario controllo » effettuato sulla firma digitale. Diversa soluzione è prospettata da A. GRAZIOSI, *op. cit.*, pp. 510-512, che individua nell'istituto dell'esperimento giudiziario *ex* art. 261 c.p.c. il mezzo per « verificare, tramite, ripetizione nel processo, se la procedura di controllo che una parte allega aver avuto esito positivo fuori dal giudizio possa effettivamente aver dato quel risultato »; ritenendo, in tal modo, che la scrittura privata informatica costituisca una prova costituenda (v. spec. p. 510 e nota 64).

Circa l'assunzione delle prove, in senso generale, v. M. TARUFFO-E. SILVESTRI, voce *Istruzione (diritto processuale civile)*, in *Enc. giur. Treccani*, XVIII, Roma, 1997, p. 11; M. TARUFFO, voce *Prova (in generale)*, in *Dig. disc. priv. sez. civ.*, XVI, Torino, 1989, p. 28; L.P. COMOGLIO, voce *Istruzione e trattazione nel processo civile*, in *Dig. disc. priv. sez. civ.*, X, Torino, 1989, p. 235.

6. (Segue) La querela di falso.

Il documento informatico munito di firma digitale ha, dunque, come si è in precedenza argomentato, l'efficacia della scrittura privata legalmente riconosciuta; ne consegue che esso forma piena prova della provenienza delle dichiarazioni da chi l'ha firmato digitalmente, fino a querela di falso[36].

La forza probatoria che l'ordinamento riconosce alla firma digitale non può essere contestata tramite il semplice disconoscimento della stessa (*ex* artt. 214, 215 c.p.c.), in quanto il valore di prova legale può, nel nostro ordinamento, essere contestato e superato soltanto tramite querela di falso[37] (*ex* art. 221 c.p.c.).

[36] Medesima conclusione è raggiunta da A. Gentili, *Documento informatico e tutela dell'affidamento*, cit., p. 174; G. Finocchiaro, *Documento informatico e firma digitale*, cit., pp. 984, 985; A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, cit., p. 517. Si precisa, infatti, che « se il soggetto contro il quale il documento digitalmente firmato è prodotto potesse disconoscerlo, la controparte dovrebbe sostenere il gravissimo onere di provare non solo che il documento informatico proviene dal presunto sottoscrittore, circostanza già provata dalla validazione della firma digitale, ma anche che egli ne è materialmente l'autore, cioè che egli ha effettivamente utilizzato la propria chiave privata per apporre la firma digitale » (così G. Finocchiaro, *op. cit.*, p. 984). In questo modo, inoltre, si addosserebbe « alla parte che produce il documento informatico un onere probatorio quasi diabolico » (A. Graziosi, *op. cit.*, p. 516) in quanto essa sarà costretta ad addurre « una prova puramente negativa dell'insussistenza di abusi o illeciti di terzi, sostanzialmente impossibile o quasi da dare », mentre, si consente alla parte che disconosce il documento informatico con firma digitale « di esimersi invocando l'abuso senza provarlo » legittimando, così, una forte sperequazione tra le parti (A. Gentili, *op. cit.*, p. 173). Cosicché « la semplice utilizzazione della firma digitale vincola colui al quale essa è riferibile a quanto discende dal documento informatico salva la possibilità di proporre contro tutto ciò una « querela di falso » nella quale più che il falso rileva l'abuso perpetrato da terzi del codice informatico, rigorosamente privato » (Id., *op. cit.*, p. 174).

Ad analoga conclusione sostanziale perviene R. Zagami, *La firma digitale tra soggetti privati nel regolamento concernente « Atti, documenti e contratti in forma elettronica »*, cit., pp. 920-923, che, però, vi giunge in diversa maniera osservando che la « mancata sottoscrizione » verificandosi solo nelle ipotesi di cui all'art. 10, comma 5, D.P.R. 513, fa sì che « il rischio dell'impiego abusivo della chiave privata da parte di persona diversa dal titolare è posto sempre a carico di quest'ultimo sul quale grava una forma di responsabilità oggettiva. Si pone, così, una presunzione assoluta di riferibilità della firma digitale al soggetto titolare della chiave pubblica che risulta dal relativo certificato ». Dunque « pur riconoscendo al documento informatico l'efficacia di scrittura privata *ex* art. 2702 c.c. non si ammette il principio di disconoscimento previsto dallo stesso articolo », precisandosi che « se si considera la verifica positiva della firma digitale, come equivalente al « riconoscimento » della sottoscrizione di cui all'art. 2702 c.c., potrebbe sostenersi in base alla stessa norma (richiamata dall'art. 5, comma 1, D.P.R. 513) l'ammissibilità della querela di falso ». Analoga conclusione si rinviene, di recente, in M. Bianca, *Diritto civile, 3*, Milano, 2000, *Il contratto*, p. 306, secondo cui « il titolare della chiave privata non può quindi disconoscere la firma digitale corrispondente alla propria chiave perché essa è giuridicamente la ''sua'' firma ».

[37] L'orientamento dominante della dottrina e della giurisprudenza è, appunto, quello di ritenere non proponibile la querela di falso contro una scrittura privata non riconosciuta o non legalmente considerata come riconosciuta (in questo senso, infatti, V. Denti, voce *Querela di falso*, in *Noviss. dig. it.*, XIV, Torino, 1969, p. 664: « la querela di falso è ammessa contro la scrittura privata soltanto nei limiti previsti da detta norma (art. 2702 c.c.); in quanto, cioè, si tratti di contestare la prova della provenienza della dichiarazione, conseguente al riconoscimento (o all'autentica-

Per un ulteriore chiarimento di questo profilo non appare del tutto irrilevante o inopportuno tenere in considerazione alcuni approfondimenti della letteratura giuridica in materia di documento[38].

Si è così osservato che al fine della legittima formazione di un documento[39] la teoria analitica della dichiarazione[40] ritiene necessarie e coessenziali le fasi dell'espressione e dell'emissione; di conseguenza anche il ca-

---

zione, o alla verificazione) della sottoscrizione »; ID., *Querela di falso e scrittura privata*, in *Scritti in onore di Carnelutti*, VI, Padova, 1950, p. 385 ss.; S. SATTA, *Commentario al codice di procedura civile*, II, *Processo di cognizione*, Milano, 1956, p. 193; L. MONTESANO, *La tutela giurisdizionale dei diritti*, in *Trattato di diritto civile diretto da Vassalli*, XIV, 4, Torino, 1985, p. 127. In giurisprudenza v. Cass., 24 febbraio 1983, n. 1420, in *Giur. it.*, I,1, 1983, c. 869; Cass., 22 settembre 1981, n. 5162, in *Rep. Foro it.*, voce *Falso (querela di)*, c. 1037, n. 3. *Contra* REDENTI, *Diritto processuale civile*, II, Milano, 1985, p. 360.

[38] Principali punti di riferimento in materia di documento sono F. CARNELUTTI, voce *Documento (Teoria moderna)*, in *Noviss. Dig. it.*, VI, Torino, 1968, p. 86 ss.; A. CANDIAN, voce *Documentazione e documento (Teoria generale)*, in *Enc. dir.*, XIII, Milano, 1964, p. 579 ss.; C. ANGELICI, voce *Documentazione e documento*, in *Enc. Giur. Treccani*, XI, Roma, 1989, p. 1 ss.; N. IRTI, *Sul concetto giuridico di documento*, in *Riv. trim. dir. proc. civ.*, 1969, p. 484 ss.; V. DENTI, voce *Prova documentale (dir. proc. civ.)*, in *Enc. dir.*, XXXVII, Milano, 1964, p. 713 ss.; G. VERDE, voce *Prova documentale*, in *Enc. giur. Treccani*, XXV, Roma, 1989, p. 11; L. CARRARO, *Il diritto sul documento*, Padova, 1941, p. 6; E.T. LIEBMAN, *Manuale di diritto processuale civile*, II, 1, Milano, 1956, p. 106; S. PATTI, *Della prova documentale*, cit., p. 4; F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, cit., p. 61.

[39] Per documento, a tal proposito, si intende il c.d. documento dichiarativo (contrapposto a quello c.d. narrativo) che è il documento in grado di rappresentare quel particolare fatto che è una dichiarazione proveniente da chi ha formato il documento stesso: quindi, può essere considerato come tale, soltanto, il documento che, oltre a rappresentare la dichiarazione, rappresenta anche il soggetto da cui proviene. Ossia il documento che contiene anche la prova della sua provenienza soggettiva, la quale coincide, com'è ovvio, con la prova della sua formazione. Il documento dichiarativo, la cui nozione coincide con quella di scrittura privata che si desume dall'art. 2702 c.c., in definitiva, contiene due dichiarazioni: l'una principale e l'altra di assunzione di paternità della prima. Così A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, cit., pp. 487, 500, 505, che su questo tema richiama, segnatamente, F. CARNELUTTI, *Lezioni di diritto processuale civile*, II, Padova, 1926, p. 481; ID., *Sistema di diritto processuale civile*, I, Padova, 1936, p. 694; ID., *La prova civile, parte generale*, Milano, 1915, pp. 158, 145; ID., voce *Documento (Teoria moderna)*, cit., p. 86, secondo cui, appunto, « un gruppo di fatti documentabili, che ha grande importanza, sono le dichiarazioni del documentatore; sotto questo profilo si distinguono nella massa dei documenti i documenti dichiarativi; tutti gli altri (non dichiarativi) si possono chiamare narrativi ».

[40] P. SCHLESINGER, voce *Dichiarazione (teoria generale)*, in *Enc. dir.*, XII, Milano, 1964, p. 374, analizzando la struttura della dichiarazione conclude che per la sua sussistenza sono essenziali un comportamento dichiarativo costituente la fase espressiva, ed una condotta complementare, costituente la fase emissiva, diretta a rendere la formula, cioè la dichiarazione, accessibile ai terzi. La fase dell'espressione non è, quindi, sempre rilevante e non è mai, di per se stessa, sufficiente, in quanto la struttura della dichiarazione ruota su due poli immancabili: un testo ed una congruente condotta diretta alla sua utilizzazione sul piano sociale, poli che si implicano reciprocamente e vicendevolmente si condizionano. L'analisi di ogni dichiarazione deve, allora, sempre svolgersi su due piani da tener ben distinti: da un lato, occorre affrontare i problemi che riguardano « il testo », cioè la dichiarazione, dall'altro, i problemi che riguardano l'*iter* procedurale cui è subordinata la rilevanza della formula elaborata . Anche G. OPPO, *Titolo incompleto e titolo in bianco*, in *Riv. dir. comm.*, I, 1951, p. 12 ss., spec. p. 20, nota 22 e p. 16, nota 11, sottolinea la necessità di scindere la dichiarazione dal documento, in quanto aver scritto non significa aver dichiarato.

rattere dichiarativo della scrittura, cioè, il suo essere emanata volontariamente dal soggetto ritenuto *ex lege* autore della stessa, deve essere provato[41]. In genere si reputa che la sottoscrizione, quindi anche la firma digitale, non faccia parte della dichiarazione, cioè della fase espressiva, ma rientri, senz'altro, nel comportamento dichiarativo di cui, anzi, costituisce un momento essenziale nel procedimento della fase emissiva[42]. Così, al fine di raggiungere *assoluta certezza* circa la paternità di un documento è indispensabile che entrambe le « operazioni », cioè l'espressione e l'emissione del documento, siano compiute dallo stesso soggetto, cioè da colui che presuntivamente viene ritenuto l'autore della scrittura.

La teoria in questione, formulata in seguito all'analisi del documento tradizionale, prospetta gli enunciati, dianzi, descritti. Questi, pur se inerenti al documento tradizionale, risultano ancor più aderenti alla realtà ed alla natura del documento informatico sottoscritto digitalmente. In questa fattispecie, infatti, il momento emissivo e quello espressivo sono ancor più distinti e separati in forza del nesso, prettamente oggettivo, intercorrente tra dichiarazione e firma digitale. Il « segno identificativo » dell'autore del documento informatico (cioè la firma digitale) attribuisce il documento al suo autore in maniera totalmente « oggettiva », attraverso, cioè, l'associazione artificiale che lega un soggetto — il titolare delle chiavi crittografiche — al proprio *instrumentum* di firma (cioè la chiave privata), che può essere utilizzato anche da persona diversa da quella collegata a tale *instrumentum*.

L'eventuale dissociazione materiale tra l'*instrumentum* di firma ed il suo titolare (in caso di uso abusivo del primo da parte di soggetti non autorizzati) non fa, però, venir meno il collegamento oggettivo fra il soggetto titolare dell'*instrumentum* e l'*instrumentum* stesso. Tra queste due entità, infatti, corre una relazione di natura esclusivamente oggettiva e non soggettiva, in forza della quale non può assumere alcun rilievo l'identità soggettiva del reale utilizzatore dell'*instrumentum*. L'utilizzazione di quest'ultimo, indipendentemente dal soggetto agente, perfezionerà la fase emissiva del documento, individuando, presuntivamente, con una sorta di evidenza pubblica come autore di tale fase il soggetto titolare dell'*instrumentum* di firma, senza che assuma alcun rilievo un'eventuale dissociazione soggettiva tra titolare dell'*instrumentum* e reale utilizzatore dello stesso. Ciò è dovuto, oltre al motivo (di ordine logico) dell'associazione artificiale ed oggettiva tra *instrumentum* di firma e suo titolare anche e soprattutto a precise e forti indicazioni legislative (art. 1, lett. *f*, D.P.R. 513; art. 1, lett. *a*, D.P.C.M. 8 febbraio 1999).

Il legame prettamente oggettivo tra chiave privata e suo titolare fa sì che un eventuale esame della firma digitale non consenta di risalire al reale utilizzatore dell'*instrumentum* di firma, poiché tra quest'ultimo e il segno

---

[41] Così, M. ORLANDI, *L'imputazione dei testi informatici*, cit., p. 875.

[42] Così P. SCHLESINGER, voce *Dichiarazione (teoria generale)*, cit., p. 378, nota 44, secondo cui in caso di documento, già completo e sottoscritto, dai caratteri dell'attività di espressione esula « tutto ciò che non riguardi la scelta e la predisposizione materiale di simboli linguistici; dalla quale, in particolare e specialmente, esula la condotta di chi sottoscrive un documento » che, dunque, confluisce nel momento emissivo, essenziale, quanto quello espressivo, nella struttura della dichiarazione, che deve, necessariamente essere costituita sia dalla fase espressiva che da quella emissiva, le quali, dunque, sono fasi tra loro distinte e complementari.

identificativo che con esso si appone corre, esclusivamente, un rapporto di natura oggettiva ed artificiale, incapace di fornire prove concrete circa l'identità del reale utilizzatore dell'*instrumentum* (mentre una sottoscrizione tradizionale è in grado, attraverso la personalità della grafia, di individuare, per illazione, l'autore effettivo del segno identificativo).

Ciò posto, appaiono razionali le soluzioni adottate dal nostro legislatore, che ha prescritto una quasi assoluta riferibilità del documento informatico firmato digitalmente al titolare della chiave privata con cui quella firma digitale è stata apposta. La riferibilità della firma digitale apposta e verificata con chiavi crittografiche non scadute, revocate o sospese al titolare delle stesse viene meno, infatti, nelle sole ipotesi descritte dall'art. 10, comma 5, D.P.R. 513; qualora, cioè, si verifichi una circostanza oggettiva, in grado di accertare che i soggetti interessati erano a conoscenza del fatto che l'associazione tra chiavi crittografiche e loro titolare era venuta meno. Fuori da tale ipotesi come autore della fase emissiva si individua, necessariamente, il soggetto collegato all'*instrumentum* di firma, cioè il titolare delle chiavi crittografiche usate, rispettivamente, per apporre e verificare la firma digitale.

Per determinare l'autore di un documento non è sufficiente individuare, soltanto, chi ha perfezionato la fase emissiva, ma è indispensabile, anche, accertare se colui che appare essere il soggetto che ha portato a termine la fase emissiva, sia anche colui che, concretamente, ha perfezionato il momento espressivo.

È, dunque, solo nel momento in cui viene accertata la corrispondenza tra il soggetto che ha « espresso » e il soggetto che ha « emesso » che si raggiunge la certezza assoluta circa la paternità del documento. In ultima analisi, il documento informatico munito di firma digitale, che individua come autore della fase emissiva, sempre e in ogni caso (salva l'ipotesi di cui all'art. 10, comma 5, D.P.R. 513), il titolare delle chiavi crittografiche, può essere ritenuto non autentico se, e solo se, il *titolare* delle chiavi *provi* che egli non sia stato l'autore della fase espressiva. Solo se, dunque, dimostri che egli non abbia posto in essere quelle dichiarazioni, che il sistema gli attribuisce *ex lege* con una sorta di « evidenza pubblica » e che la firma digitale apposta con la sua chiave privata sia il risultato dell'uso illecito della sua chiave, cioè che essa sia stata utilizzata, abusivamente, da terzi non autorizzati.

La prova in questione, potrà essere fornita, soltanto in seguito ad esperimento di querela di falso contro il documento informatico con firma digitale da parte del soggetto contro cui tale documento è prodotto e che risulta essere, *ex lege*, autore dello stesso[43].

---

[43] La necessità di esperire querela di falso contro un documento informatico sottoscritto digitalmente e, quindi, l'impossibilità di superare l'efficacia probatoria dello stesso tramite il suo disconoscimento, da parte del soggetto contro cui tale documento è prodotto, può desumersi, anche, da un ormai consolidato orientamento giurisprudenziale espresso emblematicamente da Cass., 18 giugno 1980, n. 3880, in *Giust. civ. Mass.*, 1980, p. 6: « la querela di falso e il disconoscimento della scrittura privata sono istituti preordinati a finalità diverse e del tutto indipendenti tra loro »; il secondo investe la provenienza del documento ed è volto a impedire che la scrittura acquisti l'efficacia di una scrittura legalmente riconosciuta, negando l'autenticità della sottoscrizione della scrittura, onde impedire che all'apparente sottoscrittore di essa venga imputata la dichiarazione sottoscritta. Mentre « allorché

Ciò che, in concreto, dovrà essere provato dal titolare delle chiavi crittografiche è, necessariamente, l'uso abusivo del suo *instrumentum* di firma, cioè l'illecito utilizzo da parte di terzi non autorizzati della chiave privata. Egli potrà, così, ottenere la pronuncia dell'organo giudicante che statuisca la falsità di quel documento informatico in quanto la fase espressiva è stata posta in essere da un soggetto diverso da quello che *ex lege* si presume essere l'autore della fase emissiva.

La costruzione proposta risulta, poi, coerente con l'opinione che distingue l'oggetto della verificazione da quello del giudizio di falso. La verificazione, ha per oggetto, unicamente, l'autenticità della sottoscrizione, cioè la provenienza del documento, e non già l'autenticità e, quindi, la provenienza della dichiarazione, che forma, invece, l'oggetto, esclusivo, della querela del falso[44].

---

sia accertata l'autenticità della sottoscrizione, chi voglia contestare la provenienza delle dichiarazioni contenute nella scrittura da colui che, ormai incontrovertibilmente, l'ha sottoscritta, ha l'onere di proporre querela di falso ».

Tale *incontrovertibilità* riferita alla sottoscrizione tradizionale consegue, soltanto, se ricorra una delle condizioni normative delineate dall'art. 2702 c.c.; invece, in relazione alla firma digitale tale *incontrovertibilità* consegue, semplicemente, all'esito positivo della verifica della firma digitale, poiché quest'ultima, se valida, è, già da questo momento, attribuita *ex lege* al titolare delle chiavi crittografiche.

Tale principio giurisprudenziale pronunciato in relazione alla scrittura privata tradizionale, può, *mutatis mutandis*, in rapporto alla scrittura privata informatica essere espresso nel senso che, l'*incontrovertibilità* circa il fatto della provenienza del documento informatico (si noti bene del documento e non della dichiarazione), essendo, già raggiunta, in forza della presunzione di riferibilità dell'art. 1, lett. *f*, D.P.R. 513, al momento della verifica positiva della firma digitale allo stesso apposta (ai sensi dell'art. 1, lett. *c*, D.P.R. 513), non potrà più essere contestata e, specialmente, non potrà il documento informatico con firma digitale essere disconosciuto. Infatti il dato relativo all'autenticità della firma e, quindi, quello relativo alla provenienza del documento informatico, in seguito a verifica positiva della firma digitale, se sono di natura incontrovertibile, sono non contestabili tramite disconoscimento (*ex* artt. 214, 215 c.p.c.) e, di conseguenza, non verificabili successivamente, *ex* art. 216 c.p.c.

Un elemento che, invece, non ha, ancora, assunto carattere d'*incontrovertibilità* è quello relativo alla provenienza della dichiarazione, che, in forza del principio giurisprudenziale qui riportato e, anche, di precise indicazioni dottrinarie (v. nota 44), può essere contestato, soltanto, tramite querela di falso. Questa, dunque, risulta essere l'unico mezzo processuale in grado di contrastare la forza probatoria del documento informatico munito di firma digitale, dato che la provenienza dello stesso viene stabilita *ex lege*, attraverso la presunzione dell'art. 1, lett. *f*, D.P.R. 513, che assolve la stessa funzione delle condizioni normative di cui all'art. 2702 c.c. e che, dunque, fa venir meno la *ratio* del disconoscimento e, conseguentemente, della verificazione (in quanto, ciò che con il primo si nega e con la seconda si accerta assume, già, prima della fase giudiziale, valore incontrovertibile *ex lege*). Non rimane, allora, alcuna possibilità di disconoscere l'autenticità della sottoscrizione e, quindi, la provenienza del documento informatico munito di firma digitale. Resta, soltanto, la possibilità di denunciare l'autenticità delle dichiarazioni, quindi, la provenienza delle stesse, esclusivamente, attraverso querela di falso.

[44] Così V. DENTI, voce *Querela di falso*, cit., p. 663, che, con vigore, sostiene la « radicale diversità dei due giudizi » affermando che il « giudizio di falso concerne la provenienza della dichiarazione, mentre l'altro, il giudizio di verificazione concerne la provenienza del documento »; egli disattende la contraria opinione che concepisce la querela di falso e la verificazione di scrittura come le due facce della stessa medaglia (ID., voce *Verificazione della scrittura privata*, cit., p. 765). Lo stesso autore precisa, in altra sede, che « la divergenza fra i due giudizi ha la sua ragion d'essere nella diversa natura delle situazioni che formano l'oggetto dei giudizi » (ID., *Querela di falso e scrittura privata*, cit., p. 397) « essendo funzione del giudizio di verificazione di scrittura soltanto quella di addivenire ad una sorta di « autenticazione giudi-

7. (Segue) L'Opponibilità della firma digitale.

Un ulteriore fondamentale quesito consiste nell'accertare se il documento informatico posto in essere abusivamente, cioè tramite illecito utilizzo della chiave privata da parte di terzi, possa, in seguito alla prova dell'abuso, essere opposto a chi risulta essere l'autore del documento stesso.

Ci si chiede, cioè, se il titolare di una coppia di chiavi crittografiche, provando detto abuso, possa sottrarsi alle conseguenze giuridiche derivanti dal documento informatico, di cui è, appunto, data la prova dell'illecita creazione. Ovvero, se il titolare, anche in seguito alla prova dell'uso illecito della sua chiave privata (addotta, esclusivamente, mediante querela di falso), debba, comunque, sopportare le conseguenze giuridiche, discendenti dal documento informatico, pur se abusivamente firmato con la sua chiave privata.

Tale quesito sarà risolvibile non in base ai princìpi generali ed alle regole comuni tradizionalmente intesi. Essi, infatti, in relazione al documento informatico e alla firma digitale, non possono essere meramente adattati a queste nuove realtà senza osservare quanto vi è di nuovo e di diverso rispetto alle fattispecie che, di consueto, disciplinano; ciò in considerazione della diversità dei rischi e dei vantaggi che conseguono dall'uso del documento informatico e della firma digitale.

Appare, allora, necessario un vero e proprio « *ripensamento* » di tali princìpi generali e di tali regole comuni, specie se esso sembra trovare fondamento e giustificazione nel tessuto normativo da cui emergono elementi capaci di giustificare tale scelta interpretativa[45].

Una prima conferma è, allora, individuabile nel disposto dell'art. 9, comma 1, D.P.R. 513, in cui si prescrive di « adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri », sancendo, così, specifici obblighi di protezione dei terzi. Così da evitar loro danni derivanti da un'illecita utilizzazione della chiave che induca il terzo a far affidamento, senza sua colpa, sulla dichiarazione e sulla provenienza della stessa da colui cui è riferibile la firma digitale.

Fino a che punto, poi, tali doveri vincolino il titolare della chiave privata (a quanto discende dalla dichiarazione contenuta nel documento informa-

---

ziale » della sottoscrizione, quale presupposto » del valore di prova legale della scrittura privata ai sensi dell'art. 2702 c.c. (Id., voce *Querela di falso*, cit., p. 663; ma v. anche Id., *Verificazione di scrittura e giudizio di appello*, in *Riv. dir. proc.*, 1958, p. 114; Id., *La verificazione delle prove documentali*, Torino, 1957, p. 163 ss). Sostiene la diversità della funzione e dell'oggetto dei due giudizi anche S. Satta, *Commentario al codice di procedura civile*, cit., p. 180 ss., spec. pp. 188, 190, 194 e, in un certo senso, L. Montesano, *La tutela giurisdizionale dei diritti*, cit., pp. 126, 129, 130. Di opposta opinione è invece, E.T. Liebman, *L'oggetto del processo civile di falso*, in *Riv. trim. dir. proc. civ.*, 1957, p. 602 ss., spec. pp. 602, 606; F. Carnelutti, *Teoria del falso*, Padova, 1935, p. 100, secondo il quale « tanto l'uno quanto l'altro di questi procedimenti hanno il medesimo oggetto: verità o falsità della prova »; A. Scardaccione, *Le prove*, in *Giur. sist. civ. e comm.* diretta da Bigiavi, Torino, 1971, p. 216 ss.

Per un'accurata ricostruzione dei vari modi di concepire il rapporto della scrittura privata con la querela di falso e con il giudizio di verificazione, v. G. Verde, voce *Prova documentale (diritto processuale civile)*, cit., pp. 11-13.

[45] In questo senso A. Gentili, *Documento informatico e tutela dell'affidamento*, cit., *passim*, spec. pp. 171, 174, 179.

tico firmato digitalmente) viene indicato da un'altra norma del regolamento.

L'art. 10, D.P.R. 513 ai commi 3, 4, 5 sancisce, infatti, il principio dell'univoca referenza della firma al suo titolare; subordina la validità della chiave privata alla circostanza che la chiave pubblica non risulti scaduta, revocata o sospesa; specifica che la revoca o la sospensione hanno effetto dal momento della pubblicazione, salvo che non si dimostri che esse erano già a conoscenza di tutte le parti interessate[46].

Tale norma conferma, così, il principio per il quale la chiave privata è collegata, necessariamente, con « una sorta di evidenza pubblica » al suo titolare. E che tale, esclusivo e formale collegamento viene meno, da un lato, nel caso in cui sia pubblicato il provvedimento di sospensione o di revoca della chiave pubblica, dall'altro, nel caso in cui il titolare delle chiavi crittografiche fornisca la prova che la revoca o la sospensione, comunque motivate e ancorché non pubblicate, erano già a conoscenza di tutte le parti interessate. Entrambi questi casi raffigurano *circostanze oggettive* e conoscibili, che, quindi, escludono l'affidamento dei destinatari. Questi, dunque, sembrano essere gli unici casi in cui l'abuso è opponibile ai destinatari ed in presenza dei quali il titolare della chiave privata, utilizzata abusivamente, è liberato da quanto discende dal documento informatico di cui è stata accertata l'illecita formazione da parte del titolare stesso.

In ogni altro caso, quindi, l'abuso, pur provato tramite querela di falso, non potrebbe essere opposto a terzi dal titolare delle chiavi crittografiche.

La firma digitale, infatti, per il suo regime di attribuzione, sembra vincolare, pressoché in ogni caso, il soggetto cui è univocamente riferibile, tutelando, così, in massima misura l'affidamento dei destinatari.

Da tale quadro emerge la forza logica e giuridica di una specifica ed intrinseca proprietà della firma digitale, cioè il suo pressoché assoluto « non ripudio »[47].

La sua introduzione enfatizza ed amplifica il significato e il valore giuridico, tradizionalmente, assegnati a due princìpi generali del nostro ordinamento che, nel contesto del documento informatico, assumono un rilievo decisivo in quanto sembra che essi siano, addirittura, assunti dal legislatore come criteri e canoni guida nell'emanazione delle regole relative al documento informatico.

Ad essi, dunque, è necessario ricorrere quando si debba chiarire il significato di queste regole, che debbono, quindi, essere necessariamente interpretate alla luce di detti « princìpi guida », i quali corrispondono a due « classici » princìpi fondamentali del nostro ordinamento. Essi in relazione

[46] Si vedano in, proposito, A. GENTILI, *Documento informatico e tutela dell'affidamento*, cit., pp. 175, 176, e R. ZAGAMI, *La firma digitale tra soggetti privati nel regolamento concernente « Atti, documenti e contratti in forma elettronica »*, cit., p. 921, secondo cui « come correttivo di queste gravi conseguenze è ammessa una limitata forma di pubblicità di fatto, per cui, è consentito provare (l'onere incombe su colui che chiede la revoca o la sospensione) che la revoca o la sospensione erano già a conoscenza delle parti interessate, anche in mancanza della necessaria pubblicazione, ma non anche della mancata previa richiesta di revoca o sospensione al certificatore stesso; inoltre, sembra che non sia consentito dimostrare la semplice conoscibilità della revoca o sospensione, cioè l'ignoranza dipendente da colpa ».

[47] Nel dibattito internazionale si parla di « *repudation* » con riferimento alla possibilità di respingere l'imputabilità giuridica del documento informatico firmato digitalmente con la chiave privata del soggetto che accerta l'abusivo utilizzo della stessa.

al documento informatico assumono, tuttavia, un significato nuovo e più incisivo di quello che viene loro assegnato tradizionalmente, così da assumere un valore ed un ruolo più penetranti e di primaria importanza.

Tali princìpi, come « ripensati » nel contesto del documento informatico, sono quello dell'affidamento[48] e quello dell'autoresponsabilità[49].

L'importante valore del primo è testimoniato e confermato dalla norma contenuta nell'art. 10, comma 5, D.P.R. 513, in base alla quale, come già rilevato, la firma digitale conserva la propria efficacia, quindi determina l'imputazione del documento con essa contrassegnato al relativo titolare, pur se apposta abusivamente, fino a quando non venga pubblicato, da parte del certificatore, il provvedimento di sospensione o di revoca della relativa chiave, salvo che nelle more di tale pubblicazione, il titolare delle chiavi crittografiche provi che i motivi della revoca o della sospensione erano già a conoscenza di tutti gli interessati; fino a quando, dunque, i terzi non sono posti in grado di conoscere l'inefficacia della chiave.

Il peculiare vigore del principio dell'autoresponsabilità nel « mondo » del documento informatico viene desunto, invece, dal contenuto di altre norme del D.P.R. 513.

Appare allora utile, a tal proposito, sottolineare che, negli artt. 2, 9, comma 1, il legislatore utilizza il termine « *chiunque* »[50]. Enfatizzando l'utilizzo di questo termine si può far discendere, dalla prima regola, un'ulteriore conferma della vincolatività pressoché assoluta, salvo i limitati casi di possibile ripudio (cioè quelli di cui all'art. 10, comma 5, D.P.R. 513) del documento informatico cui è apposta una firma digitale, anche in seguito alla prova della sua illecita creazione; dalla seconda regola, che prevede un'ipotesi di responsabilità da utilizzo di strumenti informatici e telematici, discende un parametro valutativo della diligenza richiesta[51], non solo al certificatore, ma, anche, all'utente privato, molto alto, rigido e rigoroso[52]. Cosicché, necessariamente, spetta a « chiunque » si voglia avvalere del sistema crittografico asimmetrico apprestare le *rigorose* « misure » del caso, idonee ad evitare danno a terzi e denunciare, tempesti-

---

[48] Sul delicato tema dell'affidamento si vedano, tra gli altri, R. Sacco, voce *Affidamento*, in *Enc. dir.*, I , Milano, 1958, p. 661 ss.; Id., voce *Apparenza*, in *Dig. disc. priv., sez. civ.*, I, Torino, 1987, p. 353; V. Pietrobon, *Errore, volontà e affidamento nel negozio giuridico*, Padova, 1990; Id., voce *Affidamento*, in *Enc. giur. Treccani*, I, Roma, 1988; A. Moschella, *Contributo alla teoria dell'apparenza*, Milano, 1973; G. Marini, *Promessa e affidamento nel diritto dei contratti*, Napoli, 1995. Si vedano altresì E. Betti, *Teoria generale del negozio giuridico*, in *Tratt. dir. civ.* diretto da Vassali, XV, 2, Torino, 1960, p. 147; F. Santoro Passarelli, *Dottrine generali del diritto civile*, cit., p. 147 ss.; M. Bianca, *Diritto civile*, 3, *Il contratto*, cit., p. 24 s.

[49] In materia di « autoresponsabilità » oltre agli autori citati nella nota precedente cfr., in particolare, il contributo di S. Pugliatti, voce *Autoresponsabilità*, in *Enc. dir.*, IV, Milano, 1959, p. 452 ss., spec. p. 461 s.

[50] Art. 2, D.P.R. 513: « il documento informatico da *chiunque* formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento ». Art. 9, comma 1, D.P.R. 513: « *chiunque* intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ».

[51] In questo senso, anche, G. Finocchiaro, *Documento informatico e firma digitale*, cit., p. 981, che sottolinea « l'assonanza con l'art. 2050 c.c. » dell'attività richiesta dall'art. 9, comma 1, D.P.R. 513.

[52] Cfr. F. Delfini, *Il D.P.R. 513/1997 e il contratto telematico*, cit., p. 295, nota 14.

vamente, all'autorità competente eventuali motivi di revoca o sospensione della validità delle predette chiavi[53].

In conclusione, la disciplina in esame si rivela improntata ai princìpi di autoresponsabilità e di affidamento, *« ripensati » in modo più rigoroso* rispetto alle ipotesi tradizionali. Essa, pur in questa nuova prospettiva e pur prestando il dovuto rilievo al principio dell'apparenza, non può essere comunque intesa fino al punto da rendere, in questa sede, assolutamente irrilevanti regole fondamentali del nostro ordinamento, che in relazione alla figura del contratto impongono, con vigore, che esso si perfezioni in forza della presenza del « consenso » delle parti e che richiedono nei confronti dell'atto in genere la sussistenza della « volontà » di chi ne è l'autore[54].

Ebbene, dire che un documento informatico cui è apposta abusivamente una firma digitale è idoneo a vincolare il titolare della chiave privata illecitamente utilizzata sino a giungere ad affermare la validità e la piena efficacia dell'atto di cui è espressione rappresenterebbe una palese violazione

[53] Numerose « regole tecniche », specificate nel D.P.C.M. 8 febbraio 1999, sono finalizzate a garantire e a tutelare il principio dell'affidamento dei terzi e a rafforzare quello di autoresponsabilità. Infatti, la stessa definizione di « dispositivo di firma » (art. 1, lett. *d*, D.P.C.M. 8 febbraio 1999) dispone che esso debba essere « in grado almeno di conservare in modo protetto le chiavi private ». Le regole relative alla « generazione delle chiavi » (art. 5, D.P.C.M. 8 febbraio 1999) cercano, poi, di garantire, nella misura più elevata possibile, « l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata », disponendo, a tal fine, specifiche prescrizioni (comma 2, lett. *a*, *b*, *c*) e richiedendo requisiti di sicurezza assai elevati, anche, rispetto ad altre leggi straniere (comma 3).

Ma, soprattutto, l'art. 8, D.P.C.M. 8 febbraio 1999 (« conservazione delle chiavi ») che, specificando l'obbligo imposto dall'art. 9, comma 1, D.P.R. 513, detta ed individua determinati obblighi per il titolare delle chiavi crittografiche. Essi, pur non esaurendo il contenuto dell'obbligo di cui all'art. 9, comma 1, D.P.R. 513, impongono specifici comportamenti ai titolari delle chiavi crittografiche per eliminare, il più possibile, il rischio di uso abusivo della chiave privata (art. 8, comma 4, D.P.C.M. 8 febbraio 1999 secondo il quale si deve « conservare con la *massima diligenza* la chiave privata e il dispositivo di firma che la contiene al fine di garantire l'integrità e la massima sicurezza; conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui (il titolare) abbia perduto il possesso o difettosi »).

Al fine di garantire, ancor più, la corrispondenza tra titolare della chiave privata ed effettivo utilizzatore della stessa, per rafforzare, così, l'affidamento dei destinatari del documento informatico munito di firma digitale, si prescrive, inoltre, una specifica procedura per la « generazione e la verifica della firma digitale » (art. 10, D.P.C.M. 8 febbraio 1999; specificamente, il comma 4 dispone che « prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all'identificazione del titolare ». Si cerca, in tal modo, di corroborare il principio di affidamento oltre che tramite il sistema crittografico asimmetrico, anche, tramite metodi d'identificazione dell'identità personale, che si presume coincidano con le c.d. chiavi biometriche di cui all'art. 1, lett. *g*, D.P.R. 513).

[54] Pur sottolineandosi, infatti, che l'affidamento è direttamente collegato, nel suo modo di operare, al destinatario di una dichiarazione e che esso comporta uno spostamento dell'interesse « dal soggetto che emette l'atto al soggetto che ne prende conoscenza » non si misconosce, tuttavia, la sua connotazione bilaterale in quanto esso è rivolto a tutelare non soltanto la fiducia del destinatario ma anche la legittima aspettativa del dichiarante: sulla bilateralità dell'affidamento v. F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, cit., p. 229; E. BETTI, *Teoria generale del negozio giuridico*, cit., p. 106; V. PIETROBON, *L'errore nella dottrina del negozio giuridico*, Padova, 1963, p. 261; M. BIANCA, *Diritto civile, 3, Il contratto*, cit., p. 394.

dei fondamentali princìpi che sono alla base della disciplina dell'atto in genere e del contratto in particolare (non tenendosi nel dovuto conto l'imprescindibile distinzione tra « documento » e « atto documentato » i quali soggiacciono a discipline, assolutamente, differenti)[55].

Pertanto un « documento » informatico con firma digitale abusiva può venire a configurarsi, sulla base della ricostruzione delle circostanze in cui l'abuso si è verificato, come espressione di un « atto » privo del consenso del soggetto che si presume esserne l'autore e che, in applicazione dei princìpi generali, può incorrere in una situazione di invalidità e, quindi, non essere idoneo a produrre gli effetti suoi propri.

Il documento informatico di cui sia dimostrata la falsità della firma digitale può, però, ancora produrre effetto nei confronti del titolare delle chiavi; il principio dell'affidamento, infatti, che, in maniera più pregnante rispetto alle ipotesi tradizionali, tutela il destinatario e i terzi affidatari può legittimare la nascita di un obbligo risarcitorio in capo al titolare della chiave privata usata abusivamente.

Si potrebbe, così, adombrare una possibile dissociazione[56] tra effetti dell'atto — venuti meno in ragione della sua invalidità — e gli eventuali

---

[55] Sul punto v. anche M. BIANCA, *Diritto civile, 3, Il contratto*, cit., p. 310, secondo cui « la formula legislativa che dichiara validi e rilevanti i contratti formati in via telematica va riferita al documento e solo di riflesso ai negozi ivi rappresentati, i quali saranno giudicati validi se e in quanto si tratti di atti a forma libera o per i quali è richiesta la scrittura privata ».

[56] Medesima conclusione, pur seguendo diversa via, è stata raggiunta da R. ZAGAMI, *Valore giuridico della firma digitale e conclusione telematica del contratto*, relazione al convegno « Documento informatico, firma digitale e commercio elettronico », Università di Camerino, 29-30 ottobre 1999, p. 10 s., in *Atti del convegno* (in corso di stampa), e in http//utenti.tripod.it/complaw/, secondo cui gli effetti dell'atto potrebbero essere eliminati a seguito del positivo esperimento della querela di falso, mentre, gli obblighi risarcitori sussisterebbero indipendentemente dall'invalidità della firma. La querela di falso, esperita dal titolare della chiave privata con cui è stata apposta la firma digitale, « potrebbe essere bloccata dalla prova del terzo affidatario incolpevole, che l'uso abusivo della chiave è stato determinato da un comportamento negligente del titolare, producendosi gli effetti della *rappresentanza apparente imputabile*. In tal senso, applicando i princìpi della firma digitale, si potrebbe affermare che l'onere di dimostrare l'apparenza è assolto dal terzo semplicemente esibendo la firma digitale, e quindi, che il titolare deve dimostrare la reale situazione contraria all'apparenza ». Secondo questo autore, inoltre, « l'apparenza non rileva se il terzo conosceva o avrebbe potuto conoscere con la normale diligenza che la firma è stata apposta da persona diversa dal titolare o eccedendo l'autorizzazione; la buona fede del terzo si presume. Se è dichiarata la falsità, entra in gioco un profilo risarcitorio nei confronti del terzo che ha riposto affidamento. Infatti, il titolare della chiave, ai sensi dell'art. 9 d.P.R. 513/1997, è tenuto al risarcimento dei danni cagionati dall'uso della chiave. In base a tale norma dovrebbe spettare a suo carico l'onere di provare di avere adottato tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ... Al terzo, che ha riposto un affidamento, secondo i princìpi generali, spetterà fornire la prova del danno ricevuto e del nesso di causalità tra attività ed evento ».

Anche secondo M. BIANCA, *Diritto civile, 3, Il contratto*, cit., pp. 306, 307, nei confronti dei terzi di buona fede trova « applicazione il principio dell'apparenza imputabile, operante nel nostro ordinamento come principio di diritto effettivo. In applicazione di tale principio il rischio della dissociazione tra paternità del documento e paternità della dichiarazione grava sul titolare della chiave... Rispetto ai terzi di buona fede l'atto vale quindi come proveniente dal titolare della firma digitale apposta al documento ». Mentre « all'utilizzatore della chiave potrà sempre essere eccepito che il documento ha un contenuto stilato contro la volontà del titolare della chiave o in difformità delle sue istruzioni ».

obblighi risarcitori, legittimati dalla tutela dell'affidamento incolpevole del destinatario e dei terzi affidatari e dagli obblighi imposti dall'art. 9 D.P.R. 513.

In sostanza, il titolare di una chiave privata usata abusivamente che dimostri, in seguito a querela di falso, l'illecito utilizzo della stessa, sarà liberato dagli effetti dell'atto ma non dagli obblighi risarcitori, i quali potranno essere eliminati solo se il titolare provi, anche, di aver adottato tutte le misure tecniche ed organizzative che l'art. 9 D.P.R. 513 impone.

La soluzione, dianzi, prospettata sembra riuscire a temperare, in modo equilibrato e nel rispetto dei princìpi dell'ordinamento, le diverse esigenze dei soggetti coinvolti in una fattispecie di firma digitale apposta abusivamente, rispondendo così, anche, ad esigenze di ordine equitativo.