V. Rizzo (a cura di), "Documento informatico, firma digitale e commercio elettronico"
Collana ITTIG-CNR, Serie "Studi e documenti", n. 2, Napoli, ESI, 2000, pp. 117-134

Valore giuridico della firma digitale e conclusione telematica del contratto

RAIMONDO ZAGAMI[1]

SOMMARIO: *1. La firma digitale quale fonte di certezze giuridiche - 2. Il ruolo delle terze parti fidate nel sistema della firma digitale - 3. A) La scrittura privata informatica - Intervento della terza parte fidata per la certificazione delle chiavi - 4. Segue: uso ed abuso della chiave privata - 5. B) La scrittura privata informatica autenticata - Intervento della terza parte fidata per la certificazione delle firme - 6. Segue: atti pubblici notarili.*

1. LA FIRMA DIGITALE QUALE FONTE DI CERTEZZE GIURIDICHE

La firma digitale è una tecnologia matematico-informatica che si propone di realizzare nel documento informatico le stesse funzioni tradizionalmente soddisfatte dalla sottoscrizione nel documento cartaceo. Norma eminente in tal senso è l'art. 10 comma 2 del D.P.R. n. 513/1997, secondo cui «L'apposizione o l'associazione della firma digitale al documento informatico *equivale alla sottoscrizione* prevista per gli atti e documenti in forma scritta su supporto cartaceo». Tale "equivalenza" è da riferirsi solo alle *funzioni* della sottoscrizione (indicativa, dichiarativa e probatoria), ma non anche ai suoi *requisiti*, i quali sono invece profondamente diversi tra sottoscrizione cartacea e firma digitale.

L'"equivalenza" tra firma digitale e sottoscrizione cartacea conduce di conseguenza all'attribuzione al documento informatico della stessa efficacia probatoria tradizionalmente riconosciuta al documento cartaceo nelle sue varie forme. E così l'art. 5 comma 1 del D.P.R. n. 513/1997 stabilisce che «Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile»; l'art. 16 comma 1 dello stesso D.P.R., che «Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato»; non vi è ancora alcun riconosci-

[1] rzagami@notariato.it

mento legislativo dell'atto pubblico notarile "originale" in forma informatica.

Dal punto di vista della tecnologia, una firma digitale è un codice informatico più o meno lungo (circa 100 caratteri), risultato dell'applicazione di un procedimento di cifratura asimmetrico (algoritmo) e di una chiave privata ad un documento informatico. La verifica dell'autenticità di una firma digitale si effettua applicando lo stesso algoritmo di cifratura asimmetrico, unitamente alla chiave pubblica correlata alla chiave privata originariamente utilizzata per la firma. Si usano, infatti, coppie di chiavi di cifratura, formate da una chiave privata con cui si appone la firma e da una correlata chiave pubblica con cui si verificano le firme già apposte.

La firma digitale, a seguito della verifica, offre soltanto due (relative) certezze: in primo luogo, che la firma è stata calcolata impiegando la chiave privata corrispondente a quella pubblica utilizzata per la verifica; in secondo luogo, che il documento informatico firmato non è stato modificato dal momento del calcolo della firma stessa (*integrità*). Scrivo "relative" certezze, perché è noto che la sicurezza di una firma digitale dipende dalla robustezza del sottostante sistema di cifratura e, dunque, non è *impossibile* falsificare una firma, bensì solo *estremamente difficile*, richiedendosi straordinarie capacità di calcolo e lunghissimi tempi di elaborazione. La sicurezza di un procedimento di cifratura è, peraltro, direttamente proporzionale alla lunghezza delle chiavi utilizzate.

Di per sé la verifica di una firma digitale non è in grado di offrire alcuna risultanza probatoria riguardo *all'identità* del soggetto sottoscrittore (la provenienza del documento). La correlazione tra chiave pubblica e chiave privata è, infatti, soltanto di tipo matematico. Diversamente, una sottoscrizione cartacea, eventualmente a seguito di verificazione, consente di stabilire un collegamento immediato e diretto tra sottoscrizione stessa e soggetto sottoscrittore.

La sottoscrizione cartacea è un dato somatico e personale, che risulta in un segno diverso per ogni soggetto che l'appone. La firma digitale, invece, non è un dato somatico, in quanto risulta dall'applicazione di un dato informatico (la chiave privata), un mezzo tecnico astrattamente utilizzabile da chiunque, in modo del tutto analogo ad un sigillo. L'analogia con un sigillo è ancora più pregnante qualora si consideri che la chiave privata è memorizzata in un dispositivo di firma che, presumibilmente,

consisterà in una carta dotata di memoria e microprocessore (*smart card*). Proprio per sottolineare questa peculiarità e differenza, nel breve dibattito che ha preceduto l'emanazione del D.P.R. n. 513/1997 si è sostenuta l'opportunità di parlare di "sigillo informatico", piuttosto che di "firma digitale" (MICCOLI). Pertanto, firme digitali apposte da soggetti diversi sullo stesso documento, utilizzando la stessa chiave e lo stesso algoritmo, non sono tra loro tecnicamente distinguibili.

Il problema è, dunque, quello di stabilire un legame tra la firma digitale apposta ed il soggetto firmatario; tra il documento informatico ed il suo autore. In altri termini, determinare il soggetto autore della firma digitale a seguito della sua verifica.

2. IL RUOLO DELLE TERZE PARTI FIDATE NEL SISTEMA DELLA FIRMA DIGITALE

Il *pieno collegamento soggettivo* tra la firma digitale ed il soggetto firmatario si realizza con l'intervento di una terza parte fidata ed imparziale in due distinte fasi.

A) In primo luogo, occorre stabilire un legame tra la coppia di chiavi ed un'identità soggettiva. Questo legame può essere posto solo mediante l'intervento della terza parte fidata che *certifica* la titolarità della coppia di chiavi in capo ad un determinato soggetto previamente identificato (art. 9 comma 2 lett. *a* D.P.R. n. 513/1997).

In realtà, tale certificazione può riferirsi solo alla chiave pubblica e non anche a quella privata, dato che la prima è di per sé correlata alla seconda. Non è quindi necessario, ai fini delle risultanze della firma digitale, che il certificatore conosca la chiave privata.

La certificazione della chiave pubblica è contenuta in un documento informatico definito come certificato, a sua volta firmato digitalmente dalla parte emittente. Il certificato è emesso preliminarmente ed è poi valido per una moltitudine successiva ed indeterminata di firme, salvo una sua cessazione di validità (scadenza, sospensione o revoca).

La terza parte fidata che certifica le chiavi, secondo la scelta normativa italiana, è un soggetto che deve rivestire la forma di società per azioni e deve rispondere a stringenti requisiti per essere iscritto in un apposito elenco pubblico tenuto dall'AIPA (art. 8 D.P.R. n. 513/1997).

La verifica di una firma digitale compiuta con una chiave pubblica certificata consente di ottenere un'identità soggettiva cui ricollegare la chiave stessa e dunque la firma. Si può così affermare con (relativa) certezza che la firma digitale verificata sia stata apposta con la chiave privata di titolarità del soggetto che risulta dal relativo certificato.

Si badi bene, con la certificazione della chiave non si ha la certezza che Tizio, titolare della chiave come risulta dal certificato, ha apposto la firma utilizzando la correlata chiave privata; bensì soltanto che la firma stessa è stata apposta utilizzando la chiave privata di titolarità di Tizio. Tecnicamente non si può conoscere *l'autore* della firma, ma solo il soggetto *titolare* della chiave. Resta incerto se la chiave privata sia stata utilizzata realmente da Tizio nell'apporre la firma o se, invece, non sia stata utilizzata concretamente da Caio.

Si ribadisce, infatti, che la chiave privata è un dato informatico, uno strumento tecnico, contenuto in una *smart card*, utilizzabile astrattamente da chiunque. Una firma digitale non essendo un dato somatico è sempre uguale (se apposta con la stessa chiave e sullo stesso documento) e, quindi, correttamente (matematicamente) verificabile, anche se apposta da soggetti diversi.

Così, nello scambio di dichiarazioni telematiche, il destinatario - oppure chi verifica un documento *ex post* - non può avere la certezza che la firma digitale che riceve, ancorché verificata con un certificato valido (non scaduto e non revocato o sospeso), sia stata effettivamente apposta dal titolare della chiave.

Le regole tecniche approvate con D.P.C.M. 8 febbraio 1999 stabiliscono che «il dispositivo di firma deve procedere all'identificazione del titolare» (art. 10 comma 4), negando così l'uso della chiave ad una persona diversa. Presumibilmente si tratterà di una *smart card* protetta da un codice segreto come un PIN o una *password*. Questo codice non è inattaccabile; inoltre, è concepibile una cessione volontaria della chiave ad altri, con la comunicazione del codice, oppure una sua decifrazione mediante attacco al cifrario.

Si sostiene che le tecniche di riconoscimento biometriche, basate sulle caratteristiche fisiche della persona (ad es. impronte digitali, impronta della retina, codice genetico, ecc.), sarebbero in grado di attribuire alla firma digitale quella caratteristica di somaticità e personalità che le manca, avvicinandola (o parificandola) alla sottoscrizione cartacea. Il D.P.R.

n. 513/1997 definisce il concetto di "chiave biometrica" (art. 1 lett. *g*) e rinvia, poi, alle regole tecniche per disciplinarne l'eventuale uso (art. 3 comma 3). Le regole tecniche emanate non contengono però ancora espliciti riferimenti all'impiego di tecniche di riconoscimento biometriche; nell'art. 8 comma 4 lett. *b* si parla piuttosto di «informazioni di abilitazione all'uso della chiave privata».

L'eventuale impiego dei dati biometrici quale strumento per l'accesso alla chiave privata, non renderebbe, comunque, "personale" o "somatica" la firma digitale, nel senso di come tale requisito si intende per la sottoscrizione.

I dati biometrici, come anche i PIN e le *passwords*, hanno la stessa funzione di strumento di controllo per l'accesso ai sistemi informatici (*simple authentication* secondo la raccomandazione ITU X.509), nel caso specifico per limitare l'uso del mezzo tecnico (cioè la chiave); e si contrappongono alla firma digitale che consente di creare documenti di cui sia possibile verificare *ex post* integrità e provenienza (*strong authentication* secondo la raccomandazione ITU X.509). Di per sé, il dato biometrico non consente di stabilire alcun legame tra un soggetto ed un documento, dato che non dipende dal contenuto del documento, ed è riutilizzabile.

I sistemi di riconoscimento biometrici presuppongono una digitalizzazione del dato fisico oggetto di esame e la sua archiviazione per servire quale termine di confronto al momento della richiesta di accesso. Non può quindi essere escluso il rischio di sottrazioni, falsificazioni, abusi ed in generale di aggiramenti del sistema di riconoscimento biometrico o di decifrazione della chiave. Con una metafora, la situazione è analoga alla conservazione di un sigillo (la chiave) in una cassaforte apribile con un codice segreto, che può essere rappresentato da un semplice PIN o da un insieme di numeri più complessi (la rappresentazione digitale del dato biometrico di riferimento). Al contrario, una sottoscrizione tradizionale, pur con tutte le difficoltà ed incertezze di accertamento, è un segno grafico che è concettualmente ed intrinsecamente diverso per ogni soggetto.

Pur riconoscendo l'elevatissimo grado di sicurezza dei sistemi di riconoscimento biometrici, resta il fatto che concettualmente non sono in grado di fornire alla firma digitale quel carattere di somaticità e personalità che le manca.

B) Occorre, quindi, risolvere questo secondo problema del legame tra la firma digitale concretamente apposta ed un'identità soggettiva.

L'unico sistema per stabilire un legame (relativamente) certo tra la firma digitale concretamente apposta e l'identità soggettiva del reale firmatario è, ancora una volta, l'intervento certificatorio di una terza parte fidata.

Essenzialmente, questa terza parte fidata assiste di persona alla concreta apposizione (generazione) della firma sul documento informatico e ne certifica il fatto, previa identificazione soggettiva del firmatario, con l'emissione di apposita certificazione a sua volta firmata digitalmente. Per cui, a seguito della successiva verifica, si potrà avere la (relativa) certezza dell'autore della firma e non soltanto del titolare della chiave.

Questo tipo di certificato è definito dalle *Digital Signature Guidelines dell'American Bar Association* (1996) e dal *Digital Signature Act* dello Utah (1995-1996), come *Transactional certificate* (o anche *attesting certificate*, o *notarial certificate*) per contrapporlo ai certificati prima esaminati (che, invece, collegano la chiave pubblica al soggetto), definiti come *Identifying certificates* (certificati di identità). Rispetto ai certificati d'identità, i certificati di attestazione devono essere emessi dopo la relativa firma digitale, hanno un contenuto diverso e, per loro natura, sono certificati riferibili ad un singolo atto (mentre un *identity certificate* si riferisce ad un numero indefinito di futuri atti); non hanno un *operational period*, cioè non hanno inizio, né fine di validità; non rileva neanche la revoca o sospensione, dato che si basano su una singola (o più transazioni) e non su un periodo di tempo di validità.

La normativa italiana sulla firma digitale accoglie sostanzialmente la figura del *Transactional certificate* e la inquadra nell'ordinamento preesistente configurandola come un'autenticazione di firma, ed assegnandone la responsabilità primariamente al notaio, quale terza parte fidata ed imparziale.

Ai sensi dell'art. 16 del D.P.R. n. 513/1997, il notaio garantisce la reale identità della parte che sottoscrive con firma digitale utilizzando la chiave privata (funzione propria del *Transactional certificate*); inoltre, indaga la volontà del sottoscrittore, realizzando la cosiddetta funzione di adeguamento; ed, infine, esegue il controllo di legalità e di conformità all'ordinamento giuridico dell'atto autenticato.

Negli Stati Uniti, in coincidenza con l'introduzione di queste nuove tecnologie, si è avvertita la necessità di istituire la nuova figura professionale del cosiddetto *Cybernotary*, delineata ufficialmente in una Risoluzione

dell'*American Bar Association* del 2 agosto 1994 e, poi, successivamente implementata per la prima volta nello Stato della Florida con legge del 30 maggio 1997. Il *cybernotary* innesta in un ordinamento di ***common law*** una funzione notarile propria del notariato di tipo latino, avendo egli il compito non solo di certificare l'apposizione della firma digitale, ma anche di assicurare la legalità dei documenti destinati all'estero (***authentication***), affinché essi non siano respinti dall'ordinamento destinatario, costituendo, pertanto, un ponte tra due tradizioni giuridiche.

A questo punto, si tratta di accertare quale efficacia probatoria possiede il documento informatico con firma digitale, a seconda che si sia realizzato l'intervento della terza parte fidata solo nella prima fase (certificazione della chiave), od anche nella seconda fase (autenticazione della firma).

3. A) La scrittura privata informatica - Intervento della terza parte fidata per la certificazione delle chiavi

Il documento informatico con firma digitale verificabile con una chiave pubblica certificata ha l'efficacia probatoria di scrittura privata ai sensi dell'art. 2702 c.c. (art. 5 comma 1 D.P.R. n. 513/1997).

L'attribuzione dell'efficacia di scrittura privata al documento informatico comporta la possibilità di compiere in tale forma gli atti per i quali è richiesta la forma scritta *ad substantiam* (art. 1325 n. 4 c.c.) o *ad probationem* (art. 2725 c.c.). In tal modo il legislatore ha ritenuto che il documento informatico con firma digitale soddisfi gli scopi perseguiti con l'imposizione di una forma vincolata: a) *ponderatezza*, cioè richiamare l'attenzione delle parti sull'importanza dell'atto che si accingono a compiere; b) *documentazione*, cioè produzione di un documento idoneo a fissare nel tempo il compimento dell'atto al fine di maggiore certezza (funzione probatoria) e di conoscibilità (strumenti pubblicitari) tra le parti e per i terzi.

Poiché il documento informatico (art. 1 lett. *a* D.P.R. n. 513/1997) è idoneo ad essere rappresentato non solo per testi, ma anche immagini, filmati, suoni ed in generale qualunque informazione digitalizzabile, ne deriva la configurabilità di *scritture private non testuali*. In perfetta applicazione del regolamento non si può negare che costituisca scrittura privata *ex* art. 5 comma 1 e soddisfi così letteralmente e sostanzialmente i requi-

siti richiesti dall'art. 1350 c.c., un documento informatico, (eventualmente anche autenticabile *ex* art. 16), recante la registrazione digitale audio e video (completabile pure con elementi testuali) della conclusione di un negozio (da trascrivere mediante indicizzazione non automatica del contenuto). Nuove prospettive si aprono anche per la forma del testamento, per cui, accanto a quello olografo, potrebbe così assumere valore quello nuncupativo.

Secondo il D.P.R. n. 513/1997, affinché per il documento informatico si realizzi l'efficacia probatoria della scrittura privata, è sufficiente l'intervento della terza parte fidata solo nella prima fase (certificazione delle chiavi) e non è richiesto l'intervento della terza parte fidata anche nella seconda fase (autenticazione della firma).

Attribuire al documento informatico l'efficacia probatoria di scrittura privata comporta che «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» (art. 2702 c.c., richiamato anche dall'art. 5 comma 1).

In caso di riconoscimento (*rectius* mancato disconoscimento entro i termini), la scrittura privata informatica forma piena prova. Se la scrittura è disconosciuta, può essere attivato il giudizio di verificazione (artt. 216 ss. c.p.c.), in cui l'onere della prova spetta a chi ha prodotto la scrittura informatica, il quale si limiterà a tal scopo ad esibire la relativa chiave pubblica certificata ed a richiedere la verifica tecnica della firma; l'esito positivo del giudizio di verificazione porta alla stessa efficacia probatoria ottenibile con il riconoscimento (piena prova).

Circa l'ammissibilità del disconoscimento, della verificazione e della querela di falso per il documento informatico sorgono pochi dubbi, dato l'espresso rinvio operato ai relativi istituti. Si è posto, invece, il problema se l'oggetto della prova nella *verificazione giudiziale* consiste nell'individuazione del reale *autore* della firma (colui che ha utilizzato il dispositivo), oppure più semplicemente nell'individuazione del soggetto *titolare del certificato*. In quest'ultimo senso gli orientamenti prevalenti, dato che diversamente si porrebbe a carico di chi produce la scrittura un onere probatorio eccessivamente gravoso e contro i principî. La titolarità di una firma digitale comporterebbe dunque di per sé una presunzione di responsabilità.

Una volta che (a seguito di riconoscimento o verificazione) la scrittura privata informatica acquisisce efficacia di piena prova, tale efficacia può essere contestata solo tramite il procedimento di *querela di falso* (artt. 221 ss. c.p.c.). In esso l'onere della prova spetta a colui che risulta sottoscrittore (art. 221 comma 2 c.p.c.), determinandosi così *un'inversione* rispetto al momento in cui la scrittura è prodotta (prima del riconoscimento o della verificazione).

L'oggetto del giudizio di querela di falso per la firma digitale consiste nello stabilire chi sia l'effettivo soggetto (autore) che ha apposto la firma utilizzando la chiave. Non si tratta, dunque di provare la "falsità" della firma (come differente da un preteso modello somatico), dato che la firma generata sullo stesso documento con la stessa chiave è indistinguibile, anche se la chiave è utilizzata da soggetti diversi dal titolare; bensì l'"abuso" nell'utilizzo della relativa chiave privata. A colui che è risultato titolare della chiave (a seguito della verificazione) spetta il difficile onere di provare il contrario, utilizzando ogni mezzo. È controverso se possa essere proposta la querela di falso indipendentemente dalla verificazione della scrittura.

Alla luce di quanto fin qui detto, risulta che l'efficacia della scrittura privata informatica diviene in realtà diversa e superiore rispetto all'efficacia probatoria della scrittura privata cartacea come delineata nell'art. 2702 c.c. Infatti, il giudizio di verificazione di una firma digitale sarebbe concretamente un procedimento rapidissimo ed automatico, che potrebbe ugualmente e facilmente compiere chiunque, ottenendo riscontri oggettivi senza alcuna complicata indagine grafologica. Pertanto, in realtà, la scrittura privata informatica sottoscritta con una firma digitale verificabile attraverso un valido certificato, avrebbe in sostanza, sempre e comunque, «l'efficacia di piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta». Riconoscimento e disconoscimento/verificazione sarebbero dunque, sostanzialmente irrilevanti e non più necessari. E, a differenza della tradizionale scrittura privata cartacea, si determinerebbe così sostanzialmente fin dall'inizio quell'inversione dell'onere della prova che pone a carico del titolare della firma l'onere di provarne la falsità - abuso della chiave privata.

Queste gravi conclusioni discendono, in ultima analisi, dal fatto che, secondo il D.P.R. n. 513/1997, l'efficacia probatoria (di piena prova)

della scrittura privata informatica deriva semplicemente dalla verifica di una firma digitale tramite una chiave pubblica certificata. In altri termini, secondo lo schema qui prospettato, l'efficacia probatoria è riconducibile ad un intervento della terza parte fidata solo nella prima fase (certificazione della chiave), non essendo richiesta, ai fini probatori della scrittura privata, anche una certificazione nella seconda fase dell'apposizione della firma (autenticazione), ritenendosi sufficiente garanzia l'"identificazione" del soggetto operata dal dispositivo di firma (art. 10 comma 4), unitamente all'identificazione preliminare operata dal certificatore in sede di emissione del certificato (art. 9 comma 2 D.P.R. n. 513/1997).

Resta, pertanto, incerto il soggetto che ha realmente apposto la sottoscrizione, utilizzando materialmente il dispositivo di firma. L'unica certezza che una tale firma offre, come si è detto, consiste nel fatto che sia stata apposta una firma utilizzando una chiave di titolarità di un certo soggetto, senza però poter sapere se la firma stessa sia stata realmente apposta del titolare risultante dal certificato.

Non potendo tecnicamente risultare alcuna prova circa il soggetto reale autore della sottoscrizione, l'unico sistema per attribuire efficacia probatoria a tali firme è ricorrere a dei *meccanismi presuntivi di responsabilità* in capo al titolare della chiave come risulta dal certificato. Dalla verifica di una firma digitale non risulterebbe dunque l'autore di essa, bensì più correttamente soltanto il soggetto che è responsabile per la firma apposta. Dalla titolarità di un certificato deriverebbe una presunzione di provenienza delle firme digitali con esso verificabili in capo al titolare medesimo.

Il problema è accertare se tale presunzione di provenienza (responsabilità) ammetta - ed in che misura - una prova contraria da parte del titolare della chiave certificata, per potersi sottrarre alla responsabilità derivante da una firma a lui riconducibile, ma da lui non realmente apposta. Lo strumento giuridico per contestare la sostanziale presunzione di provenienza (apposizione) della firma in capo al titolare del certificato, sembra essere, come si è detto, la querela di falso, con un difficile onere probatorio a carico dell'attore.

Un meccanismo presuntivo di questo tipo, con la possibilità espressa della prova contraria, è ad esempio previsto dal *Digital Signature Act* dello Utah.

4. SEGUE: USO ED ABUSO DELLA CHIAVE PRIVATA

Concretamente, la generazione della firma da parte di persona diversa al titolare della chiave può verificarsi in vari modi. Ad es. lo smarrimento del dispositivo di firma ed il suo utilizzo abusivo (prima della revoca), rottura del cifrario ed individuazione della chiave privata da parte di un crittoanalista, aggiramento dei sistemi di riconoscimento biometrici, falsa certificazione (nel 1999 non sono più considerate sicure le chiavi di lunghezza non superiore a 512 *bits*). Un tale comportamento è facilmente concepibile quando la *smart card* è protetta da un semplice codice, ma, come si è detto, non è del tutto escludibile anche in presenza di sistemi di riconoscimento biometrici.

Va, comunque, subito precisato che l'utilizzo di una chiave privata dopo la perdita di validità del relativo certificato, a seguito di scadenza, sospensione o revoca, «equivale a mancata sottoscrizione» (art. 10 comma 5 D.P.R. n. 513/199). Il problema si pone, pertanto, solo per le firma digitali apposte durante il periodo di validità del certificato (*operational period*). Ad es. il dispositivo di firma smarrito che è utilizzato da un impostore, prima della richiesta e pubblicazione della revoca da parte del certificatore.

Per la soluzione di questo problema occorre procedere alla ricerca di una ragionevole soluzione che soddisfi in modo equilibrato i diversi interessi coinvolti, nel rispetto del più generale quadro normativo dell'ordinamento italiano, tenendo in considerazione i seguenti fattori:

a) che il reale autore della firma potrebbe non essere identificabile (ad es. contrattazione telematica);
b) che il terzo, dalla verifica del certificato valido, ripone un affidamento che merita di essere tutelato e che la sua buona fede dovrebbe essere presunta;
c) che il titolare della chiave certificata è tenuto a rispettare dei comportamenti di diligenza nella sua custodia;
d) che il titolare della chiave certificata è entrato volontariamente (con il contratto di certificazione) in un sistema di cui era in grado di valutare anticipatamente i rischi e le responsabilità;
e) che il titolare potrebbe aver autorizzato altri ad usare la sua chiave.

La querela di falso, attivata secondo le modalità prima esposte, potrebbe essere bloccata dalla prova da parte 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 principî alla 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 della chiave deve dimostrare la reale situazione contraria all'apparenza. 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 un affidamento. Infatti, il titolare della chiave, ai sensi dell'art. 9 D.P.R. n. 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 aver adottato tutte le «misure organizzative e tecniche idonee ad evitare danno ad altri» (ad es. la cura nella custodia della chiave).

Per quanto riguarda l'utente, nella valutazione di una sua eventuale responsabilità, si dovrà tener conto degli obblighi a suo carico, consistenti nella conservazione della chiave e del dispositivo con la massima diligenza; conservazione delle informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; richiesta immediata della revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi (art. 8 comma 4 reg. tec.); nonché divieto di duplicare la chiave privata o i dispositivi che la contengono (art. 8 comma 2 reg. tec.).

Si discute se la norma dell'art. 9, comma 1, debba applicarsi al solo certificatore, oppure anche all'utente. La disposizione sembrerebbe applicabile anche agli utenti, dato che l'art. 8 comma 1 (applicabile soltanto agli utenti e non ai certificatori) presenta una formulazione in parte identica all'art. 9 comma 1 in questione. Il comma 2 dell'art. 9 è, invece, testualmente, applicabile solo ai certificatori e non anche agli utenti. La rubrica dell'art. 9 parla, inoltre, di «obblighi dell'utente e del certificatore».

Sembra trattarsi, in sostanza, di una tipizzazione della fattispecie di "responsabilità per l'esercizio di attività pericolose" prevista dall'art. 2050

c.c., come si desume anche dalla relazione ufficiale al D.P.R. n. 513/1997, che riporta anche esempi riferiti al solo utente, come l'abuso da parte di altri in mancanza di tempestiva revoca.

Al terzo, che ha riposto un affidamento, secondo i principî generali, spetterà fornire la prova del danno ricevuto e del nesso di causalità tra attività ed evento. Egli potrebbe anche fornire la prova che il titolare della chiave abbia omesso colposamente di effettuare la revoca della chiave stessa, essendo a conoscenza della sua compromissione o dell'uso abusivo.

Tuttavia, se il terzo conosceva (o era in grado di conoscere) che l'utilizzatore era persona diversa dal titolare, si verifica un'interruzione del nesso di causalità, ed il titolare non può più essere ritenuto responsabile. L'art. 1227 comma 2 c.c. (richiamato dall'art. 2056 c.c.), stabilisce, infatti, che «il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza». La prova della mala fede o della colpa del terzo danneggiato, secondo i principî generali, spetta al titolare della chiave (danneggiante), una volta che il danneggiato stesso abbia provato il nesso di causalità.

In definitiva, secondo la ricostruzione esposta, si potrebbe realizzare una dissociazione tra gli effetti dell'atto e gli eventuali obblighi risarcitori. I primi, potrebbero essere eliminati a seguito della querela di falso; i secondi, a tutela dell'affidamento dei terzi, sussisterebbero indipendentemente dall'efficacia della firma. Per la diffusione del sistema diventano indispensabili adeguati contrappesi assicurativi a garanzia dei titolari delle chiavi, analogamente a quanto accade oggi per le carte di credito.

Peraltro, le ipotesi in cui una chiave privata è utilizzata da un soggetto diverso dal suo titolare non sempre danno luogo ad abusi, contrastabili con la querela di falso, ma possono anche prospettare fattispecie meritevoli di tutela.

Si pensi alle ipotesi in cui la *smart card* è volontariamente consegnata, insieme al codice di abilitazione, ad altra persona per essere utilizzata. In tal caso è dubbio se possa parlarsi di rappresentanza diretta, essendo difficile un inquadramento nella categoria tradizionale della spendita del nome (*contemplatio domini*). La particolarità è che, in tal caso, Caio non solo agisce *in nome* e per conto di Tizio; ma agisce *con il nome* di Tizio, eventualmente senza nemmeno fare risultare il proprio nome Caio: vi è la spendita del nome del solo rappresentato, ma non anche del nome del

rappresentate; manca la cosiddetta dichiarazione di procura (incarico rappresentativo).

Allora ci si deve chiedere se esiste spazio per una nuova nozione di *contemplatio domini* valida per l'àmbito informatico che possa rispondere alle nuove esigenze e che non richieda necessariamente la dichiarazione di procura (menzione dell'incarico rappresentativo), realizzando nello stesso tempo la *ratio* a base della spendita del nome. Infatti, quando Caio utilizza la chiave di Tizio, spendendo (soltanto) il nome di quest'ultimo, non vi possono essere dubbi in capo al terzo che l'atto sia riferibile al rappresentato (Tizio), piuttosto che al rappresentante (Caio), del quale ultimo potrebbe ignorare anche il nome.

Nell'àmbito del documento informatico sono realizzabili comportamenti e fattispecie che non erano prima nemmeno concepibili. Nell'àmbito cartaceo è inconcepibile che Caio firmi con il nome di Tizio apponendo una firma che non è tecnicamente distinguibile da quella che avrebbe potuto apporre lo stesso Tizio. Questa, invece, è proprio la fattispecie in questione, facilmente realizzabile con la firma digitale, proprio in relazione a quella sua precisata caratteristica di "sigillo" informatico.

Qualora si accetti la tesi della rappresentanza diretta come sopra, la diversa e speculare ipotesi in cui l'uso della chiave altrui è compiuto senza previa autorizzazione, potrebbe essere inquadrata sotto la categoria della falsa rappresentanza, come tale suscettibile di ratifica (art. 1399 c.c.). Con riferimento alla documentazione cartacea, è stato scritto che «La sottoscrizione apocrifa [apposta da persona diversa da quella risultante dal nome sottoscritto] non è altro che una *contemplatio* non autorizzata, e produce i medesimi effetti di ogni altra spendita del nome: il diritto potestativo del contemplato alla ratifica dell'atto. Il *falsus procurator* e l'usurpatore del nome altrui si presentano come ipotesi omologhe di difetto di potere: il negozio concluso da un soggetto diverso da chi appare come titolare, presenta il requisito negativo del difetto di un potere rappresentativo» (ORLANDI).

Per fondare la responsabilità del titolare della chiave nei confronti del terzo non sembra, comunque, applicabile l'art. 1398 c.c., il quale stabilisce una responsabilità non del rappresentato (nel nostro caso il titolare della chiave), bensì del falso rappresentante, il quale potrebbe essere, nel caso in esame, non identificabile (si pensi ad es. alle contrattazioni telematiche a distanza).

5. B) La scrittura privata informatica autenticata - Intervento della terza parte fidata per la certificazione delle firme

In una prospettiva di simmetria tra documentazione cartacea ed informatica, l'efficacia probatoria della scrittura privata informatica autenticata è quella stessa stabilita per la sottoscrizione autenticata su carta dall'art. 2703 c.c. La disposizione dell'art. 16 comma 1 del D.P.R. n. 513/1997 riproduce in modo sostanzialmente identico il contenuto dell'art. 2703 c.c., e nello stesso tempo vi rinvia espressamente. La firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato «si ha per riconosciuta» (art. 16 comma 1 ed art. 2703 comma 1 c.c.) e, pertanto, ai sensi dell'art. 2702 c.c., farà piena prova della provenienza delle dichiarazioni da chi ha sottoscritto il documento informatico, anche se colui contro il quale è prodotto non riconosce la sottoscrizione, salvo l'esperibilità della querela di falso.

Sotto questo punto di vista, alla luce di quanto detto prima, le differenze tra firma digitale autenticata e non autenticata, si affievoliscono. Infatti, come si è visto, anche la firma digitale non autenticata in realtà acquisterebbe l'efficacia di far piena prova (fino a querela di falso) a seguito di un giudizio di verificazione del tutto formale, oggettivo ed immediatamente risolvibile mediante l'esibizione di una chiave pubblica certificata. D'altra parte, anche per la firma digitale autenticata occorrerebbe procedere ugualmente ad una verifica della firma digitale apposta dal pubblico ufficiale.

L'autentica o la verificazione giudiziale sono, comunque, indispensabili per l'ottenimento di un titolo per le modifiche dei registri di pubblicità legale (ad es. Registro delle imprese e Registri immobiliari). Inoltre, si ribadisce che l'intervento della terza parte fidata in sede di autentica *ex* art. 16 è l'unico strumento che fornisce la garanzia della reale identità del sottoscrittore, cioè che la firma digitale sia stata apposta spontaneamente e coscientemente dall'effettivo titolare della chiave pubblica utilizzabile per la verifica e non da altri. Inoltre, il notaio indaga la volontà del sottoscrittore ed esegue il controllo di legalità.

L'art. 16 del Regolamento, riproducendo in parte l'art. 2703 c.c., prescrive che «l'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza [art. 72 l. not.] dal titolare, previo accertamento della sua iden-

tità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte [art. 47 comma 3 l. not.] 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» (legge notarile).

In presenza di un'autenticazione *ex* art. 16 l'ipotesi che la firma sia stata apposta da un soggetto diverso dal titolare della chiave, può essere fatta valere con la querela di falso. Allo stesso modo, può essere fatta valere la falsità della firma digitale del pubblico ufficiale autenticante.

I poteri del pubblico ufficiale autenticante andrebbero dimostrati attraverso un certificato particolare della sua chiave pubblica, denominato certificato d'attribuzione, emesso e gestito in modo diverso e più sicuro dei certificati ordinari d'identità. Ai sensi dell'art. 17 comma 3 del D.P.R. n. 513/1997, «le chiavi pubbliche dei pubblici ufficiali non appartenenti alla Pubblica Amministrazione sono certificate e pubblicate autonomamente in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'àmbito dei rispettivi ordinamenti giuridici».

6. SEGUE: ATTI PUBBLICI NOTARILI

Un intervento del notaio in questa seconda fase (apposizione della firma) potrebbe essere volto alla produzione di un atto pubblico notarile. Il D.P.R. n. 513/1997 non prevede, ma nemmeno esclude, la redazione di un atto pubblico notarile *originale* in forma informatica, come è invece espresso per la scrittura privata (art. 5 comma 1).

In attesa di un intervento normativo chiarificatore, si è, pertanto, sostenuta l'ammissibilità in base al regolamento di un atto pubblico notarile in forma informatica (PETRELLI, MICCOLI, ANDRINI), adducendo vari argomenti. La legge Bassanini (e non il D.P.R. n. 513/1997) avrebbe abrogato parzialmente le norme della legge notarile - e tutte le altre norme - incompatibili con la documentazione informatica. Nel D.P.R. n. 513/1997 non è stata riproposta la disposizione dell'art. 1 comma 2 del primo progetto di legge del settembre 1996, che escludeva espressamente gli originali degli atti pubblici notarili. Diverse norme prevedono già atti pubblici in forma informatica, come ad es. l'art. 491 *bis* c.p., il quale prevede una fattispecie di falso applicabile agli atti pubblici; l'art. 3 del d. lgs. 12 febbraio 1993, n. 39, relativo alla documentazione amministrativa; e

lo stesso art. 15 comma 2 della l. n. 59/1997, relativamente agli atti amministrativi. Le formalità richieste per l'atto pubblico notarile non sarebbero incompatibili con il tipo di documentazione informatica e, comunque, parziali e letterali incompatibilità sarebbero superate da un'interpretazione evolutiva delle norme.

Al contrario, l'esclusione di un atto pubblico notarile esclusivamente in forma informatica potrebbe sostenersi con i seguenti argomenti. In primo luogo, perché, mentre è stato richiamato l'art. 2702 c.c. per la scrittura privata, ed è stato quasi esattamente riprodotto l'art. 2703 c.c. (scrittura privata autenticata), non è posta alcuna norma che tratti degli atti pubblici notarili (*ubi lex voluit dixit; ubi noluit tacuit*). In tal modo, resterebbero pienamente applicabili tutte le formalità richieste dalla legge notarile (l. n. 89/1913) e dalla l. n. 15/1968, le quali sono ancora parzialmente incompatibili con una documentazione informatica (d'altra parte il regolamento non aveva, comunque, la forza di legge per effettuare modifiche in tal senso). Inoltre, la scelta di escludere gli atti pubblici notarili avrebbe anche una sua intrinseca ragionevolezza, dato che potrebbe essere stata probabilmente determinata dal fatto di non voler estendere una tecnologia ancora nuova ed inapplicata, e pertanto "rischiosa", ad un documento che, possedendo un'efficacia probatoria privilegiata (art. 2700 c.c.), rappresenta il massimo rigore formale del nostro ordinamento, ed in quanto tale è richiesto come forma minima per atti ritenuti dal legislatore di rilevante importanza patrimoniale e personale.

D'altra parte, per la conclusione degli atti notarili, l'utilità della firma digitale è minore, dato che essi non potrebbero comunque essere conclusi telematicamente, poiché, a differenza delle scritture private autenticate, è richiesta la contestuale presenza di tutte le parti (e degli eventuali testimoni e fidefacienti) davanti al notaio per la lettura e sottoscrizione. L'utilità si ripresenta quando occorre duplicare o trasmettere telematicamente il documento pubblico già concluso. In tal senso, il D.P.R. n. 513/1997 viene in aiuto, poiché, anche a voler negare la stipulabilità di un atto pubblico notarile *originale* in forma informatica, si prevede la copia informatica di un atto pubblico che fa fede come l'originale su carta (art. 6 comma 2).

In conclusione, tutti i problemi giuridici fin qui esposti non sorgerebbero e non meriterebbero ulteriori approfondimenti se si volesse circo-

scrivere l'operatività della firma digitale a settori limitati e specifici (ad es. pubbliche amministrazioni e grandi aziende). Ma se l'intenzione è quella di estendere questo sistema alla generalità dei cittadini, per compiere la cosiddetta "rivoluzione epocale del documento informatico", non si può prescindere dal ricercare equilibrate soluzioni giuridiche che garantiscano tutte le parti coinvolte.