TEMA II

IL NOTAIO E LA CONTRATTAZIONE ELETTRONICA

Relatori: *Ugo Bechini – Michele Nastri*

CAPITOLO I

L'EVOLUZIONE DEL SISTEMA-PAESE: IL RUOLO DEL NOTARIATO

1. Premessa; 2. L'evoluzione e lo stato della normativa e del sistema; 3. I futuri sviluppi della informatizzazione della Pubblica Amministrazione italiana.

CAPITOLO II

LA FIRMA DIGITALE

1. L'adozione della firma digitale in Italia; 1.1. Thick laws e thin laws; 1.2. Il sistema a chiavi asimmetriche; 2. L'equiparazione tra firma digitale ed autografa; 2.1. Atti sottoscrivibili; 2.2. La provenienza del documento firmato; 2.2.1. I rischi di origine umana: le Autorità di Certificazione; 2.3. Solennità della sottoscrizione; 2.4. Accessibilità; 3. Il regime probatorio; 4. La delega de facto; 5. La morte del titolare; 6.1. La Direttiva 93/1999; 6.2. Il D.Lgs. 10/2002; 7. La firma digitale affonda?

CAPITOLO III

LA FIRMA DIGITALE APPLICATA ALLA FUNZIONE NOTARILE

1. Aree di impiego; 2. Riconoscibilità della funzione; *2.1 - Riconoscibilità (segue): le Certification Authorities notarili;* 3. La durata del documento informatico; *3.1 - La verificabilità nel tempo;* 4. La firma digitale: un pericolo per il notariato?

CAPITOLO IV

LE APPLICAZIONI NOTARILI

1. Software e norme; 2. La pubblicità immobiliare; 3. Pubblicità commerciale

CAPITOLO I

L'EVOLUZIONE DEL SISTEMA-PAESE: IL RUOLO DEL NOTARIATO

SOMMARIO. 1. Premessa; 2. L'evoluzione e lo stato della normativa e del sistema; 3. I futuri sviluppi della informatizzazione della Pubblica Amministrazione italiana.

1. Premessa

L'esplosione esponenziale dell'informatica, della telematica, del mondo delle reti e delle applicazioni informatiche utilizzate non più come sistema di ausilio a modalità operative e di lavoro tradizionali, ma come strumento autonomo ed autosufficiente, assume in Italia una caratterizzazione del tutto peculiare, ed in qualche modo contrastante, rispetto al tipo di sviluppo che si è verificato nel resto del mondo.

Solo partendo da questa peculiarità è possibile spiegare un fenomeno che è stato sotto alcuni aspetti più rapido e di dimensioni maggiori, ma anche in certa misura diversamente orientato, rispetto a realtà vicine ed apparentemente simili, ed arrivare a comprendere il ruolo del notariato italiano in tali vicende.

Se l'Italia è in questo momento il paese nel quale sono stati emessi in assoluto il maggior numero di certificati di sottoscrizione relativi a firme elettroniche avanzate (o firme digitali, secondo l'espressione tuttora presente nella legislazione italiana per designare il tipo di firma elettronica avente il maggior riconoscimento dall'ordinamento giuridico), occorre dar conto delle caratteristiche e delle ragioni di un simile fenomeno, soprattutto in quanto si distingue in modo netto da altre esperienze nazionali, che invece ci si aspetterebbe di trovare consimili.

Altrettanto preme affermare le ragioni, non tecnologiche, ma sociali e giuridiche, della presenza del notariato in prima linea in questa esperienza, al punto che il notariato costituisce al momento, in ambito italiano e quindi, sicuramente europeo, il gruppo di utenti della firma digitale che effettua l'uso più massiccio di tali applicazioni, come si documenterà in prosieguo[1].

Si tratta, in poche parole, di questo: mentre l'introduzione delle tecnologie informatiche prima, e telematiche poi, e tra queste in particolare della firma digitale e dei sistemi di autenticazione che consentono la contrattazione a distanza, è stata generalmente rivolta in primo luogo ad applicazioni di e-commerce, B to B (business to business) o B to C (business to consumer), e solo in seguito ad applicazioni aventi valore legale assoluto anche nel campo del diritto pubblico, in Italia si è ritenuto di utilizzare l'informatica, e l'evoluzione tecnologica in senso generale, per effettuare un rivoluzionario rinnovamento della Pubblica Amministrazione, e per superarne problematiche vecchie di decenni che avevano portato ad una sostanziale arretratezza e ad una scarsa efficienza del sistema.

Dall'inizio degli anni novanta dello scorso secolo, e con maggiore vigore dal 1997, l'Italia è infatti impegnata in uno sforzo evolutivo tendente a dotare il paese di una macchina amministrativa e burocratica all'altezza delle sfide internazionali derivanti, sul piano mondiale, dalla globalizzazione del sistema economico, ma anche, sul piano regionale, dalla progressiva integrazione economica e politica dell'Unione Europea.

[1] Cfr. infra § 2.

I mutamenti del quadro generale hanno messo in discussione il ruolo che l'amministrazione pubblica aveva nel tempo assunto, ruolo parallelo, ed in certo modo deviante, rispetto al ruolo originario di fornitura di servizi primari. L'obiettivo dell'efficienza era stato infatti via via affiancato da quello dell'utilizzazione della Pubblica Amministrazione quale strumento politico in senso lato, utile per l'assorbimento di tensioni sociali anche mediante la creazione, all'occorrenza, di posti di lavoro[2]. Il mutamento del quadro economico generale, e conseguentemente di quello politico, hanno messo in discussione un modello di Pubblica Amministrazione nel quale il livello di efficienza non elevato non risultava dannoso per la collettività nel suo complesso, ed era compensato da una funzione politica di prevenzione e soluzione di problematiche sociali.

Nel tentativo di recuperare velocemente un livello di efficienza e di competitività della Pubblica Amministrazione comparabile a quello degli altri paesi più industrializzati si è quindi iniziato un processo accelerato di informatizzazione, allo scopo di migliorare la natura e la qualità dei servizi, anche in termini di tempi di risposta, e di ridurre i costi.

Il metodo utilizzato per ottenere tali scopi è stato il graduale riconoscimento di valore giuridico pieno agli atti realizzati con strumenti informatici[3], e la creazione di strutture per introdurre l'uso di tali mezzi (l'Autorità per l'Informatica nella Pubblica Amministrazione e le successive evoluzioni di tale originario organismo, fino ad arrivare all'attuale struttura basata sul Dipartimento per l'Innovazione e le Tecnologie, retto da un Ministro).

Nel far ciò si sono ottenuti risultati in primo tempo altalenanti, in ragione di una serie di fattori che possiamo qui in qualche modo semplificare:

- la notevole frammentazione della Pubblica Amministrazione in Italia, che non può essere considerata in modo unitario se non a livello di macrocategorie, e le conseguenti differenze nei processi, nei modelli organizzativi, nel livello e quantità di strutture e personale;
- la proliferazione di una legislazione amministrativa sovrabbondante, da coordinare con normative locali (derivanti dal potere legislativo concesso alle regioni) e settoriali; la presenza massiccia della prassi amministrativa come fonte di comportamenti obbligati e la conseguente carente formalizzazione di alcuni processi usuali[4];

[2] Si pensi ai casi in cui situazioni di grave disagio sociale od occupazionale in determinate zone erano risolte mediante la creazione di apparati della Pubblica Amministrazione o, a volte, mediante la diretta assunzione di personale di aziende in crisi destinato altrimenti alla disoccupazione.

[3] La norma iniziale di questo processo è stata senz'altro l'art. 3 del D.Lgs. 39/93, con il quale è stata formalmente riconosciuta in ambito amministrativo la possibilità di sostituire alla sottoscrizione manuale l'indicazione a stampa del sottoscrittore, ed è stata superata una serie di rilevanti problematiche relative in particolare ad atti amministrativi emessi in quantità imponenti (si pensi all'irrogazione di sanzioni per infrazioni al codice della strada).

[4] Non è questa la sede per esaminare la rilevanza della prassi nel sistema della Pubblica Amministrazione Italiana. A titolo di esempio si ricorda che non si rinviene nell'intero "*corpus*" normativo vigente, una normativa che regoli la tenuta dei registri di protocollo, se si eccettua (con una assimilazione valida solo in linea estremamente generale) il repertorio notarile, utilizzato peraltro dalla legislazione (art. 67 e 68 del D.P.R. 131/86, Testo Unico dell'Imposta di Registro) e dalla prassi, quale paradigma di altri registri assimilabili. Solo la normativa sul protocollo informatico nella Pubblica Amministrazione (D.P.R. 428/1998 e D.P.C.M. 51/2000) ha dettato regole generali e comuni su questo elemento cardine dei processi interni di ogni struttura.

- l'eccessiva fiducia nel mezzo informatico, e nella sua capacità quasi "taumaturgica" di risolvere i problemi, senza passare attraverso un processo di analisi che, partendo dall'esistente e dai risultati che si intendono ottenere, adegui i processi al nuovo strumento, sfruttandone le potenzialità;
- i tempi di adeguamento delle infrastrutture di base (disponibilità di mezzi informatici quali computer, reti locali, collegamenti ad Internet od alle reti protette che via via si andavano formando) e della preparazione del personale;
- i tempi di accettazione socio-culturale dei nuovi strumenti.

Il tema principale tuttavia, sottostante a tutti i profili elencati, è senz'altro quello dell'uso di una tecnologia nata per fini diversi da quelli per cui viene effettivamente utilizzata, allo scopo di effettuare attività che, per il solo mutare del mezzo, finiscono per cambiare natura e possibili finalità, e causare rischi applicativi.

I sistemi per la digitalizzazione dell'attività di documentazione in senso generale, e tra questi in particolare quelli di firma digitale, che ne sono il fulcro, nascono nel mondo anglosassone e per l'utilizzo nell'ambito del commercio elettronico. Da una parte quindi si tratta di un'esperienza che vede la luce in ordinamenti giuridici in cui non esiste la rilevanza pubblicistica del documento così come la si intende nei paesi di cd. *civil law*, dall'altra il sistema è stato, ed è finora prevalentemente utilizzato, per finalità che prevedono un interscambio tra soggetti predeterminati, e quindi la preventiva accettazione di regole generali sulla validità ed imputabilità del documento informatico munito di firma digitale o elettronica, da parte dei singoli soggetti che ne fanno uso, nei confronti di un numero limitato di altri soggetti, ma non una validità generalizzata riconosciuta dall'ordinamento giuridico.

Tale elemento, per così dire genetico, influisce in modo non sempre congruo sulle applicazioni di firma digitale con piena validità giuridica e sui sistemi di conservazione documentale.

E' evidente infatti che un meccanismo, quale quello originario, basato sul reciproco riconoscimento tra i soggetti che ne usufruiscono, non può essere utilizzato, senza opportuni aggiustamenti, per applicazioni di firma digitale cui l'ordinamento riconosca validità giuridica *erga omnes.*

Un sistema basato sul mutuo riconoscimento tra privati viene costituito sulla predeterminazione di regole, comuni che si possono discostare dalle regole generali dell'ordinamento, e sull'accettazione delle stesse soprattutto in materia di ripartizione di responsabilità.

Non altrettanto può dirsi in caso di applicazioni con valenza pubblicistica.

Allo stesso modo la sostituzione di documenti cartacei con documenti informatici, in termini di processo originariamente basato sul documento informatico, e più ancora la sostituzione con riproduzioni informatiche di documenti originariamente cartacei, richiedono la creazione di un sistema di regole e procedimenti che individuino l'ambito applicativo, le modalità ed i responsabili. Ciò può esistere sulla base di un preventivo accordo interprivatistico nell'ambito di un gruppo chiuso di utenti, ma necessita di un riconoscimento da parte dell'ordinamento giuridico generale non appena vi siano questioni di opponibilità a terzi o, più in generale, di opponibilità *erga omnes.* Per dirla con un esempio, è perfettamente lecito che le parti di un rapporto interprivatistico convenzionalmente predeterminino le forme per lo svolgimento delle fasi dello stesso, e per i singoli atti che costituiscono le vicende di un rapporto contrattuale complesso, basandosi sul principio della libertà della forma, che si estrinseca anche nella libertà di predeterminare forme convenzionali, e che trova espressione e limite, nell'ordinamento

italiano, nella norma dell'art. 1352 c.c.[5]. Quando si tratti di un contratto per il quale l'ordinamento prevede un requisito formale (quale la forma scritta *ad substantiam* nell'ordinamento italiano per le vendite immobiliari a norma dell'art.1350 c.c.) ed entrano in gioco pertanto valutazioni del legislatore che non attengono soltanto ai profili interprivatistici del rapporto, ma anche ad aspetti di rilevanza pubblicistica, sarà necessario, per dare riconoscimento al documento informatico, avere una normativa che definisca la rilevanza sostanziale ed i profili probatori dello stesso, ed affronti le problematiche proprie del nuovo strumento, ed inesistenti nella realtà precedente, quali, ad esempio, i profili della conservazione nel tempo del documento.

In Italia ad oggi esistono, e sono costantemente utilizzate, una serie di applicazioni del documento informatico avente pieno valore legale che costituiscono allo stesso tempo frutto e fonte delle riflessioni che abbiamo cominciato ad esporre e che costituiranno oggetto di questo lavoro. Si tratta di un'esperienza, da considerare allo stesso tempo un dato acquisito ed un *work in progress*, per l'elaborazione di un sistema normativo, organizzativo ed applicativo dell'uso di documenti informatici che abbiano il medesimo valore del documento scritto, od anche dell'atto pubblico. Questa esperienza è senz'altro unica nel suo genere per ampiezza di applicazione e importanza dei fenomeni interessati, e presenta ormai in molte ipotesi le caratteristiche del fenomeno *a regime* e non semplicemente quelle del caso sperimentale *(best practice).*

In questo fenomeno il notariato italiano è stato soggetto sempre più trainante di tutte le applicazioni che di volta in volta si sviluppavano, fino ad assumere in alcuni casi il ruolo di soggetto di riferimento anche per fenomeni che non lo riguardavano direttamente, ma che potevano modellarsi sulle esperienze del notariato. Al di là delle problematiche di volta in volta affrontate, la funzione necessaria, e generalmente riconosciuta dagli interlocutori, svolta dal notariato in queste attività, è stata quella di individuare gli elementi di garanzia generale del sistema, e quindi dei diritti dei singoli e della collettività, che dovevano essere salvaguardati nel passaggio dai sistemi di documentazione tradizionale a quelli digitali, individuando i rischi propri del nuovo sistema e le garanzie necessarie, opponendosi a scorciatoie che, anche solo per l'ansia di fare, avrebbero potuto (e ancora potrebbero) mettere in gioco la certezza del commercio giuridico. Non è un caso comunque che, al di là del numero dei certificati di firma rilasciati, il maggior numero di utilizzazioni di firme digitali derivi da attività proprie del Notaio o strettamente connesse.

2. L'evoluzione e lo stato della normativa e del sistema

La descrizione dello stato di sviluppo del documento informatico in Italia non può prescindere dall'evoluzione normativa, che ne è stata costantemente motore e fonte di indirizzo, ed in qualche caso, come vedremo, freno.

Si tratta di un fenomeno che può essere compreso nei suoi sviluppi se si considera che il graduale approccio degli operatori pratici, prima alla realizzazione delle infrastrutture di base per la creazione del documento informatico, e poi alla pratica dello stesso con piena rilevanza giuridica, ha portato ad una comprensione sempre maggiore dei problemi e delle peculiarità che non possono essere affrontati se non con strumenti creati appositamente, non essendo utilizzabili quelli tradizionali. In altre parole solo

[5] Sulla norma dell'art. 1352 c.c. come parziale espressione di principi generali inespressi nel codice civile, G.MIRABELLI, *Dei Contratti in generale*, Torino, 1980, pag. 214; S.GENOVESE, *Le forme volontarie nella teoria dei contratti*, Padova, 1949, pag. 52 ss..

l'approccio alla realtà fenomenica, al di là della ricostruzione giuridica e/o dogmatica, ha consentito (*rectius* sta consentendo) di individuare in che modo le differenze ontologiche[6] del documento informatico, rispetto al documento tradizionale, incidano sulla qualificazione delle fattispecie giuridiche che lo riguardano.

Le fasi evolutive della normativa italiana costituiscono quindi la traccia di un percorso che ha coinvolto tutto il sistema, non può dirsi affatto concluso[7], e può essere un valido esempio per la pratica del documento informatico almeno nei paesi di *civil law*.

Il percorso può iniziare, dal punto di vista normativo, con l'art. 3 del D.Lgs. 39/93,[8] che per la prima volta, dopo un dibattito dottrinale durato sin dagli anni '80, introduce un concetto di documento realizzato con strumenti informatici nell'ordinamento nazionale italiano.

---

[6] Quest'aspetto è esattamente colto da G. FINOCCHIARO, La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici, in Comm. C.c. Scialoja-Branca a cura di GALGANO, Bologna, 2000, pag. 1 ss., ed ancora in Firma digitale e firma elettroniche. Il quadro normativo italiano dopo il d. legisl. 10/2002, in Contratto e Impresa, 2002, pag. 853 ss. e, specificamente, pag. 854. Ci si permetta di rinviare anche a E. SANTANGELO M. NASTRI, Firme elettroniche e sigilli informatici, anticipato in Vita Notarile, 2/2002 pag. 1124, ed ora in AA.VV. (A CURA DI F. BOCCHINI) Diritto dei consumatori e nuove tecnologie, Torino, 2003, pag. 237 ss.

[7] Cfr. infra nel testo.

[8] Comma 2: Nell'ambito delle pubbliche amministrazioni l'immissione, la riproduzione su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante sistemi informatici o telematici, nonché l'emanazione di atti amministrativi attraverso i medesimi sistemi, devono essere accompagnate dall'indicazione della fonte e del responsabile dell'immissione, riproduzione, trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile. Tale norma è stata già oggetto di diverse pronunzie della Suprema Corte (Sez. I, sent. n. 7234 del 07-08-1996, Prefetto di Genova c. Viale [rv 499014], e Sez. I, sent. n. 9394 del 24-09-1997, Pagani c. Prefetto della Provincia di Milano [rv 508214]) che confermano la possibilità, peraltro testuale, che l'atto amministrativo non sottoscritto in originale sia valido. L'ultima di tali pronunzie così ribadisce la necessità della sussistenza di diversi requisiti perché la mancanza di sottoscrizione non infici l'atto: "l'autografia della sottoscrizione non è configurabile come requisito di esistenza giuridica degli atti amministrativi, quanto meno quando i dati esplicitati nello stesso contesto documentativo dell'atto consentano di accertare la sicura attribuibilità dello stesso a chi deve esserne l'autore secondo le norme positive, come è confermato dall'art. 3 del D. Lgs. 12 febbraio 1993, n. 39, il quale, prevedendo, nel caso di emanazione di atti amministrativi attraverso sistemi informatici e telematici, che la firma autografa sia sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile, ribadisce sul piano positivo l'inessenzialità ontologica della sottoscrizione autografa ai fini della validità degli atti amministrativi. Tuttavia, di fronte alla precisa contestazione formulata sul punto dall'opponente, il pretore doveva accertare l'esistenza nell'originale del provvedimento, in mancanza della sottoscrizione del Prefetto, di quella di un suo delegato o, in caso diverso, doveva specificare le ragioni per cui, sulla base della legislazione vigente all'epoca in cui l'atto fu emanato, esso doveva ritenersi "proveniente in maniera inequivoca dall'Ufficio della Prefettura di Milano"." Tale norma, sinora non esplicitamente abrogata, non va considerata superata dalla normativa sul documento informatico, ma, in una interpretazione evolutiva, riferibile soltanto agli atti amministrativi, e tra questi agli atti che formati con strumenti elettronici siano poi portati a conoscenza dei destinatari o dei terzi sotto forma di documento cartaceo; essa ha un peculiare ambito applicativo nel settore degli atti amministrativi (come certificati, o ordinanze-ingiunzioni erogative di sanzioni amministrative) che siano in gran numero ed eventualmente con pluralità di destinatari, ma abbiano contenuto identico o similare. Nel senso di un sostanziale superamento di tale normativa M. CAMMARATA E. MACCARONE, La firma digitale sicura. Il documento informatico nell'ordinamento italiano. Milano, 2003, pag. 53 ss.,

La vera rivoluzione si verifica però con l'art. 15 della legge 59/97[9], che riconosce, sia pure con qualche incertezza lessicale che si tradurrà in dubbi interpretativi[10], pieno valore giuridico al documento informatico, e conseguentemente, alla firma digitale come unico criterio di imputazione del documento informatico pienamente riconosciuto (quale risulta dal D.Lgs. 513/1997). E' stato poi il tempo delle norme attuative, previste inizialmente come norme di carattere esclusivamente tecnico (in particolare il D.P.C.M. 8 febbraio 1999, in corso di sostituzione nel momento in cui si licenzia per la stampa

[9]Le principali norme di riferimento del settore sono le seguenti:

1) l'art. 15 comma 2, della legge 15 marzo 1997, che riconosce l'immediata efficacia del documento informatico e rimanda a norme regolamentari per i criteri e le modalità di applicazione, norme emanate con il D.P.R. 10 novembre 1997 n. 513, poi trasfuso nel D.P.R. 445/2000.

2) Il D.P.R. 28 dicembre 2000 n. 445, (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) che recepisce nel corpo del testo unico, con alcune modifiche, il D.P.R. 10 novembre 1997 n. 513; tale regolamento riuniva in sé i regolamenti previsti dalla legge 59/97. Di fatto, il T.U., ed in precedenza il D.P.R. 513, non provvede a specificare esaustivamente i "criteri e le modalità", ma definisce gli aspetti più generali della materia, rinviando (art. 8) alle regole tecniche (da emanarsi con D.P.C.M. da modificare con cadenza almeno biennale, decorrente dalla entrata in vigore del D.P.R. 513, pubblicato sulla G.U. 13 marzo 1998 n. 60) le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici;

3) le regole tecniche di cui all'art. 3 del D.P.R. 513/97 per la "formazione, trasmissione, conservazione e validazione, anche temporale" dei documenti informatici e di cui al citato art. 18 per i documenti informatici della P.A. Tali regole tecniche sono state emanate con D.P.C.M. 8 febbraio 1999, pubblicato sulla G.U. n. 87 del 15 aprile 1999, e di recente rinnovate con D.P.C.M. 13 gennaio 2004, pubblicato sulla G.U. n. 98 del 27 aprile 2004.

4) l'art. 3, comma 2, del D.Lgs. 39/93, mai abrogato, in materia di documento informatico della P.A.

5) La direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, e la normativa di recepimento nazionale prevista dalla legge 29 dicembre 2000 n. 422, e risultante dal D.Lgs 23 gennaio 2002 n. 10, e dal D.P.R. 17 aprile 2003 n. 137, che hanno apportato importanti modifiche al D.P.R. 445/2000;

6) La Direttiva 2000/31/CE del Parlamento Europeo e del Consiglio, del 8 giugno 2000 (Direttiva sul commercio elettronico) contenente alcune norme che riguardano i contratti;

7) le norme sul protocollo informatico e precisamente il D.P.R. 20 ottobre 1998 n. 428, ed il D.P.C.M. 31 ottobre 2000;

8) la normativa relativa alla conservazione del documento informatico, ad oggi costituita dalle norme del D.P.R. 445/2000 e dalla Deliberazione C.N.I.P.A. n. 11/2004 del 19 febbraio 2004.

9) la normativa relativa alla formazione e conservazione dei documenti informatici aventi rilevanza fiscale in attuazione della normativa nazionale e della Direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di Iva, e costituita dal Decreto del Ministro delle Finanze 23 gennaio 2004, (Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto).

10) la normativa sul processo telematico contenuta nel D.P.R. 13 febbraio 2001 n. 123, in attesa di ulteriori norme di attuazione.

L'elenco delle norme di riferimento del settore potrebbe allungarsi con le deliberazioni e circolari prima dell'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) oggi del C.N.I.P.A. (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), e va tenuto conto che è prevista l'ulteriore emanazione di un decreto sulla Posta Elettronica Certificata, che dovrebbe risolvere le problematiche relativa alla trasmissione ed alla recettizietà del documento informatico.

[10] E' stato ampio ed è tuttora non definitivamente risolto il dibattito circa l'applicabilità della normativa sul documento informatico ad ogni tipo di documento ivi compreso l'atto pubblico notarile. Le variazioni nel tempo della normativa hanno in qualche caso semplificato, in altri casi complicato il percorso interpretativo. Al tema, che si porrà praticamente all'attenzione del notariato nei prossimi anni, si ritiene di non poter dare una soluzione definitiva, almeno in assenza di un contesto normativo più completo. Sul punto cfr. infra nel testo, cap. 2.

questo lavoro), ma che hanno inevitabilmente definito, anche per la genericità eccessiva della normativa di rango superiore, alcune importanti tematiche giuridiche, quali i compiti del Certificatore che rilascia certificati digitali e la gestione nel tempo dei documenti informatici.

L'emanazione della Direttiva UE 93/99/CE ha costretto il legislatore italiano ad interventi notevoli per adeguare il sistema originariamente previsto, basata sul riconoscimento del valore legale alla sola firma digitale rilasciata da Certificatori iscritti ad un apposito elenco pubblico sotto il controllo dello Stato, alle multiformi ipotesi di firma elettronica previste dalla Direttiva, con un valore giuridico graduato[11].

Lo sviluppo della normativa, parallelo alle prime applicazioni, costituisce un indice delle problematiche che si sono riscontrate nella fase attuativa. In particolare il tema che ha creato i maggiori problemi, e le maggiori oscillazioni e discussioni in dottrina, è quello delle condizioni di imputabilità e disconoscimento del documento informatico, ed ha perciò subito nel tempo notevoli modifiche, e con ogni probabilità ancora ne subirà[12].

Interessa però rilevare, seguendo la linea del nostro discorso, che l'emanazione di una normativa completa – almeno nelle intenzioni - in tutte le sue parti sin dal 1999, non ha risolto tutte le problematiche, e che la reale utilizzazione della firma digitale in modo consistente non ha avuto inizio se non dopo alcuni anni ed ulteriori sforzi.

Sono infatti immediatamente sorti alcuni problemi relativi alle applicazioni della firma digitale.

Tra questi è stata rilevata in primo luogo la necessità di creare, ad un livello di maggiore specificità rispetto a quanto previsto dalle norme tecniche, una piattaforma di condivisione delle specifiche tecniche (cd. interoperabilità) che consentisse l'effettivo uso della firma digitale con validità *erga omnes* secondo le previsioni normative. Si è infatti riscontrato che l'uso, da parte dei Certificatori della firma digitale, di tecnologie fornite da diversi produttori, ed adattate dai singoli alle proprie specifiche esigenze, comportava notevoli problematiche nell'uso promiscuo di firme fornite da vari Certificatori. Il certificato di firma digitale, pur basato su *standard* internazionali, era infatti sviluppato in modo diverso dai vari produttori, così come gli strumenti per l'apposizione della firma (*hardware* e *software*) e per la verifica della validità. Ciò è perfettamente compatibile con sistemi chiusi, quali quelli del commercio elettronico, per

---

[11] Sulla distinzione tra firma elettronica, firma elettronica qualificata, firma digitale, cfr. G. FINOCCHIARO, *Firma digitale e firma elettroniche*, cit. *passim.*, U. BECHINI –M. MICCOLI – *Attuazione della direttiva europea sulla firma elettronica, ovvero la forma "sine probatione"* in *Notariato*, 3/2002, pag. 327 ss., e E. SANTANGELO –M. NASTRI, *Firme elettroniche*, cit. pag. 1126 ss..

[12] La normativa originaria in materia di firma digitale consentiva il disconoscimento della firma digitale senza limitazione alcuna, e sulle modalità a limiti del disconoscimento si sviluppo un ampio dibattito nella dottrina del settore. La riforma del D.Lgs. 10/2002 ha ritenuto di rafforzare il valore probatorio del documento informatico, riconoscendo al documento informatico munito di firma elettronica avanzata pieno valore probatorio fino a querela di falso. In entrambi i casi si può sinteticamente osservare che si onera uno dei soggetti interessati (il titolare della firma o il soggetto che vuole opporre al titolare il documento sottoscritto con firma avanzata) di una prova nella maggior parte dei casi impossibile. La coscienza di tale problematica ha spinto il legislatore italiano a prevedere in una legge delega (art. 10 della legge 29 luglio 2003 n. 229, che concede 18 mesi per l'emanazione della normativa delegata) un nuovo intervento in materia di mezzi di prova dell'imputabilità del documento informatico munito di firma elettronica. Sul tema, oltre i testi citati alla precedente nota 11, cfr. i lavori contenuti nel testo edito a cura del Consiglio Nazionale del Notariato, AA.VV. *Firme elettroniche questioni ed esperienze di diritto privato*, Milano, 2003.

i quali nasce l'applicazione della firma digitale, ma non è accettabile in sistemi, quale quello italiano, destinati ad un uso generalizzato del documento informatico munito di firma digitale ed alla sua diffusione anche a destinatari indeterminati.

D'altro canto i soggetti industriali, che si affacciavano al mercato della firma digitale con ambizioni di carattere commerciale, non erano inizialmente del tutto preparati ad affrontare un percorso di coordinamento ed omogeneizzazione delle tecnologie necessario per l'uso della firma digitale previsto dalla legislazione italiana, e pensavano forse più allo sviluppo di mercati di settore, da gestire con applicazioni proprietarie.

Una prima opera di uniformazione tecnica è stata svolta dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) che, coordinando il lavoro con i Certificatori all'epoca presenti, sul mercato ha emanato una circolare (la n. 24 del 24 giugno 2000) che costituisce il primo concreto risultato in materia di interoperabilità della firma digitale. Tale circolare non si è rivelata tuttavia uno strumento sufficiente a consentire l'effettiva realizzazione di un sistema in cui chiunque potesse utilizzare una firma digitale rilasciata da un qualsiasi Certificatore utilizzando un qualunque *hardware* e *software* di firma ed ottenendo che la firma così apposta sia verificabile con qualunque *software* di verifica. Ciò è stato realizzato, ed in piccola parte è ancora da realizzare, ad opera dei Certificatori[13] iscritti all'elenco dei Certificatori Accreditati presso la Pubblica Amministrazione italiana, attraverso un'opera spontanea di coordinamento, avvenuta a seguito della comprensione della necessità di rendere omogenei gli strumenti per consentire lo sviluppo del mercato.

Non può nascondersi però che la necessità di simili attività costituisce un'implicita critica all'operato dei legislatori, nazionale ed europeo.. Un sistema che riconosca la piena validità giuridica delle firme digitali, od elettroniche avanzate secondo la definizione della Direttiva UE, non può esimersi dall'imporre, almeno a livello di precetto normativo, il dialogo pieno ed effettivo tra le tecnologie utilizzate, in condizioni di piena fruibilità anche per utenti non professionali, e deve distribuire le responsabilità relative al rispetto di tali requisiti nell'ambito di chi produce e distribuisce le firme digitali. Ciò non è sufficientemente chiaro né nella normativa nazionale né nella normativa europea[14].

La normativa europea, ed in sede di recepimento anche quella nazionale, nell'intento di preservare la libera concorrenza attraverso il rifiuto della scelta di singole tecnologie, legittima l'uso, in materia di firma elettronica, di qualunque tipo di meccanismo, con ciò estendendo a dismisura il concetto di firma elettronica fino ad estenderlo a tecnologie che possono anche non costituire criteri di imputabilità, in quanto non riferibili ad alcun soggetto[15].

---

[13] Un ruolo importante in questo settore è stato ed è svolto dall'Assocertificatori, associazione tra i certificatori di firma digitale, costituita nel 2001, cui partecipano i principali Certificatori privati del settore industriale ed il Consiglio Nazionale del Notariato, e che svolge tra i propri scopi istituzionali, volti alla diffusione della firma elettronica avanzata, la diffusione di sistemi interoperabili. Maggiori informazioni sulle attività svolte dall'associazione sono reperibili all'URL http://www.assocertificatori.org.

[14] Sul tema della responsabilità e sulle problematiche ancora aperte M.DOLZANI, Il regime delle responsabilità. Obblighi dei soggetti interessati e spunti per un inquadramento sistematico, in AA.VV. Firme elettroniche questioni ed esperienze di diritto privato, cit..

[15] E' ciò che espressamente sancisce l'art. 5 della Direttiva 93/99/CE quando definisce la firma elettronica cd. semplice o leggera.

Né la previsione della direttiva europea di riconoscere con apposite decisioni della Commissione le norme tecniche di riferimento per prodotti di firma elettronica è andata oltre uno sporadico provvedimento, che non copre se non un settore molto limitato[16].

Il risultato di questa politica è la sostanziale indeterminatezza del settore anche commerciale della firma elettronica, e la mancanza di un mercato di settore se non a livello nazionale, sulla base di esperienze nazionali quali quella italiana.

Abbiamo quindi da una parte una normativa che definisce firma elettronica e conferisce rilevanza giuridica a meccanismi anche di scarsissima affidabilità[17], dall'altra uno sviluppo effettivo del settore (in Italia) sulle sole applicazioni riferibili alla firma digitale quale originariamente intesa dal legislatore italiano, sulla base delle esigenze riferibili ai rapporti con la Pubblica Amministrazione.

La prima utilizzazione pratica che è stata sviluppata in Italia è infatti l'applicazione di firma digitale ai rapporti con il Registro delle Imprese, che gestisce la pubblicità delle società e commerciale in genere. Ciò in virtù della logica evoluzione di un progetto che ha consentito la pratica attivazione di tale Registro[18], rimasto per un lungo periodo inattuato, attraverso la sua realizzazione direttamente con strumenti informatici e telematici. Si tratta di un chiaro esempio di quel percorso evolutivo della Pubblica Amministrazione italiana che si è inizialmente descritto.

L'alimentazione di tale registro, tuttavia, non può essere effettuata con dati forniti da chiunque, ma solo dai soggetti abilitati, ed in particolare dagli stessi imprenditori e dai notai, per quanto attiene le numerose formalità che possono essere eseguite solo se l'atto che ne costituisce titolo ha forma di atto pubblico o scrittura privata autenticata.

Identico problema si pone per l'implementazione della pubblicità immobiliare con tecniche totalmente informatiche, in quanto possono costituire oggetto della pubblicità immobiliare solo gli atti pubblici, le scritture private autenticate (e quindi atti redatti autenticati in massima parte dai notai, prevedendo l'ordinamento italiano la legittimazione alla rogazione ed all'autentica degli atti solo in capo ai notai ed a un limitatissimo novero di altri pubblici ufficiali roganti nell'interesse di pubbliche amministrazioni), ed alcuni atti del processo.

E' intuitivo, a questo punto, che simili procedure si possono attivare solo se, oltre al controllo della imputabilità del documento informatico ad un certo soggetto, è possibile verificare la sussistenza in capo allo stesso delle funzioni che abilitano il soggetto all'espletamento di tali attività.

Il Notariato italiano ha quindi posto con forza il problema dell'enunciazione di qualifiche, funzioni e poteri nell'ambito del trattamento del documento informatico. Anche in questo caso il principale problema da affrontare è stato quello dell'insufficienza degli strumenti tecnici disponibili per realizzare un'applicazione che

[16] Decisione della Commissione del 14 luglio 2003.

[17] Si può ritenere che la Direttiva costituisca un compromesso tra le esigenze dei paesi di *common* law con quelle dei paesi di *civil* law, e la firma elettronica come meccanismo di sicurezza nell'ambito del commercio elettronico con la firma elettronica con efficacia giuridica *erga omnes*.

[18] Il Registro delle Imprese era infatti previsto fin dall'entrata in vigore del codice civile del 1942, ma era rimasto inattuato. La pubblicità commerciale era rimasta regolata, in virtù di disposizioni transitorie, dalle norme del codice di commercio del 1882, e la tenuta dei relativi registri era effettuata presso le cancellerie commerciali dei Tribunali. La legge 580/1993 ha previsto l'attuazione del registro delle imprese con tecniche informatiche ed ha trasferito la competenza per la sua tenuta alle Camere di Commercio. Dal 19 febbraio 1996 è attivo tale registro, che è ormai alimentato esclusivamente alimentato con documenti informatici muniti di firma digitale, costituiti per una gran parte da copie di atti notarili. Sul punto infra § 4.

avesse tutti i requisiti previsti dall'ordinamento, e della conseguente riluttanza degli interlocutori tecnici ad affrontare la questione, che è stata, a più riprese, semplicemente negata, anche contro l'evidenza. Lasciando ad altra parte di questo lavoro l'analisi dei meccanismi astrattamente e concretamente utilizzabili[19], si può anticipare che il problema è stato risolto attraverso l'assunzione da parte del Consiglio Nazionale del Notariato del ruolo di Autorità di Certificazione iscritta all'elenco pubblico, ma dedicata esclusivamente alla certificazione delle firme digitali dei notai italiani, con garanzia quindi non solo della identità del firmatario, ma anche della sussistenza in capo allo stesso delle funzioni notarili, e con il conseguente obbligo per il titolare di utilizzare la firma digitale così rilasciata solo nell'esercizio di tali funzioni. Va detto che tale sistema, oltre ad essere attuato per il notariato, è stato in qualche modo esemplare, come testimoniano la recente assunzione del ruolo di Certificatore Accreditato, sempre in relazione a specifiche funzioni, del Consiglio Nazionale Forense (per gli avvocati, in previsione della telematizzazione delle vicende processuali), e dell'esercito (per i militari)[20]. Inoltre sono in corso prime applicazioni in esercizio, terminata la fase della sperimentazione, di altri sistemi per l'enunciazione all'interno dei meccanismi di firma digitale delle funzioni qualifiche e poteri, basati su sistemi previsti dagli standard tecnici internazionali, ma sinora di scarsa applicazione pratica[21].

Lo sviluppo e la diffusione della firma digitale si sono quindi indirizzati verso applicazioni che facilitano l'interazione nei confronti della Pubblica Amministrazione, e le difficoltà riscontrate sono tipiche di tale tipo di rapporti. Nel contempo lo sviluppo delle applicazioni di firma elettronica non connesse a tali problematiche, e più orientate quindi al commercio elettronico, ha avuto un oggettivo rallentamento, dovuto da una parte alla preferenza del mercato verso tecnologie più semplici, coniugate a sistemi di mutuo e preventivo riconoscimento, ed a limitazioni di responsabilità per quanto attiene gli aspetti economici, e dall'altra alla confusione normativa.

Un rapido cenno, prima di passare ad esaminare rapidamente lo stato della diffusione della firma digitale, merita un'applicazione tipicamente notarile, di cui si tratterà diffusamente in prosieguo[22]. Si tratta del sistema che consente l'effettuazione, in modalità quasi totalmente telematica, delle formalità di registrazione, ipotecarie e di voltura catastale degli atti notarili, attivo a partire dal 2001 ed esteso a tutto il territorio nazionale dalla fine del 2003. Questo sistema, realizzato, a partire dall'aprile 2003, attraverso l'utilizzazione della firma digitale dei notai, consente l'effettuazione di tutte le formalità dipendenti dagli atti notarili aventi contenuto immobiliare con modalità telematica, e quindi l'adempimento degli obblighi fiscali (ed i relativi pagamenti) e di quelli relativi alla pubblicità immobiliare ed all'aggiornamento dei registri del catasto. Esso, pur in attesa di completamento per l'estensione della totale telematizzazione agli atti non immobiliari, da una parte, ed alla parte più propriamente relativa all'esecuzione

[19] cfr. § 3.2.1

[20] Maggiori informazioni possono essere ottenute attraverso la consultazione dell'elenco pubblico dei certificatori reperibile all'indirizzo http://www.cnipa.it. Il Manuale Operativo dell'Autorità di Certificazione del Consiglio Nazionale del Notariato, che costituisce, unitamente al contenuto del certificato di firma, lo strumento attraverso il quale si dichiara la destinazione delle firme digitali emesse da tale certificatore esclusivamente agli esercenti le funzioni notarili, è presentato sul sito Web http://ca.notariato.it nell'area Documentazione.

[21] Un modello condiviso, che consentirebbe, a regime, un sistema di verifica automatica delle funzioni basto su un sistema di codifica, è stato realizzato, su impulso e con il contributo del Consiglio Nazionale del Notariato, da Assocertificatori, ed è reperibile sul sito http://www.assocertificatori.org.

[22] Cfr. infra § 4.2.

della pubblicità immobiliare dall'altra, costituisce da un punto di vista quantitativo l'applicazione di uso più massivo della firma digitale in ambito di piena validità giuridica.

Analizziamo quindi, sulla base delle considerazioni svolte ed allo scopo di dimostrarne la fondatezza, alcuni dati statistici sull'uso della firma digitale in Italia[23].

Il numero di certificati di firma digitale complessivamente rilasciati in Italia al 31 dicembre 2003 era pari ad 1.525.000[24].

Di tali certificati il maggior numero (circa 1.000.000) è stato distribuito dal Certificatore Infocamere società di supporto del sistema delle Camere di Commercio e quindi del Registro delle Imprese.

I certificati rilasciati dall'Autorità di Certificazione del Consiglio Nazionale del Notariato a tale data ammontano a 5.489, di cui circa l'85% ancora attivi.

Il numero delle formalità presentate telematicamente, o comunque su supporto informatico munito di firma digitale ai Registri delle Imprese per le società nel periodo luglio 2003 (data di inizio dell'obbligatorietà di tale procedura) – marzo 2004 ammonta a circa 1.000.000, di cui circa 400.000 presentate dai notai in relazione ad atti da loro rogati o autenticati[25]. Se si considera il fatto che gli atti notarili costituiscono l'unico veicolo (eccezion fatta per la piccola aliquota costituita dai provvedimenti giurisdizionali) per gli eventi costitutivi, modificativi, ed estintivi delle società, e che in tali cifre è compresa l'effettuazione dell'unico adempimento annuale obbligatorio per le società, vale a dire il deposito dei bilanci per le società di capitali, si comprende la rilevanza dell'apporto del notariato a tale procedura. Se poi si tiene conto del fatto che ciascuna pratica comporta l'apposizione della firma digitale su un numero di documenti non inferiore a due, e mediamente di almeno tre, si arriva ad una media mensile di oltre 120.000 documenti sottoscritti dai notai con firma digitale per questa applicazione.

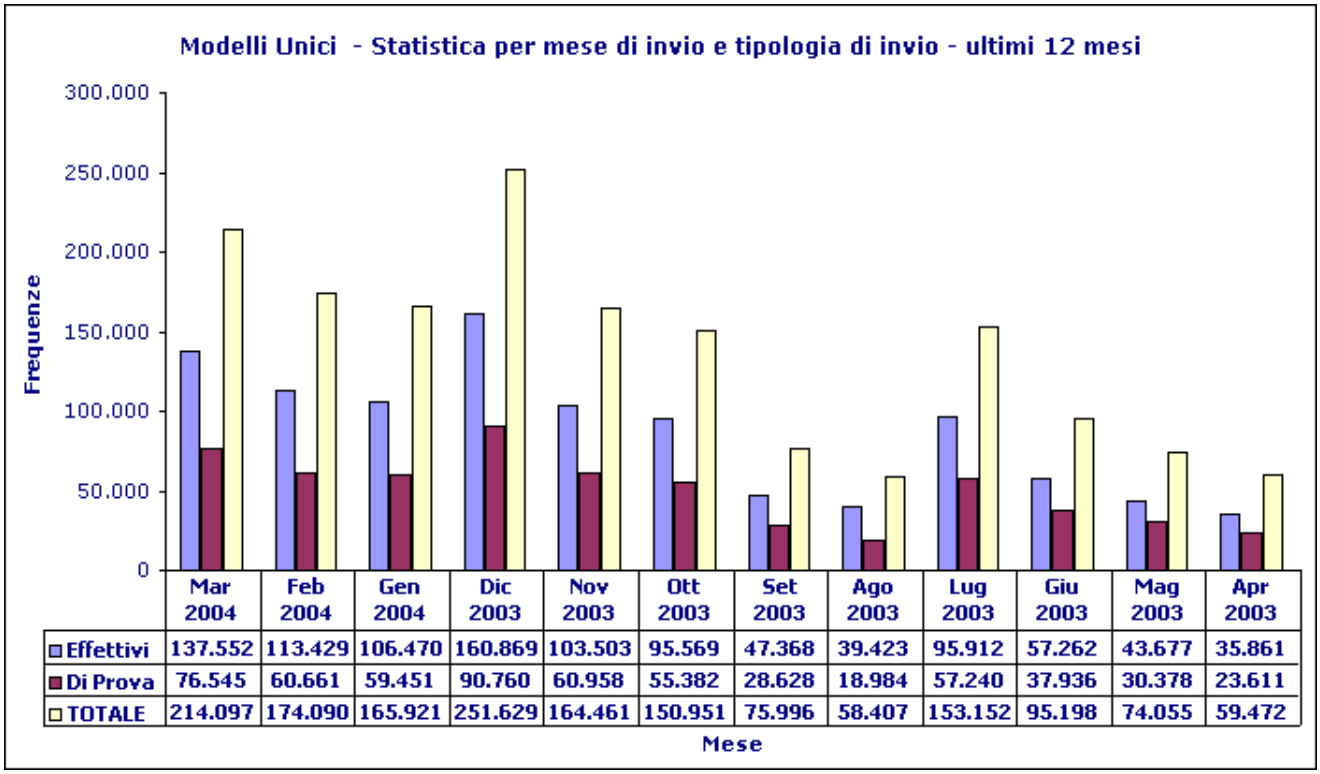
Il numero di atti notarili immobiliari registrati con modalità telematica e quindi muniti di firma digitale nel corso del periodo aprile 2003 – marzo 2004, è di 1.037.165. Nel periodo dicembre 2003 (data di estensione dell'obbligatorietà a tutto il territorio nazionale) – marzo 2004 la media mensile degli atti registrati con modalità telematica e sottoscrizione elettronica è stata di 130.000[26].

[23] Non sembra un caso, sulla base delle considerazioni svolte, l'irreperibilità di dati statistici relativi alla firma elettronica semplice.

[24] Dati forniti da Assocertificatori. Manca il numero dei certificati rilasciati da Certificatori non aderenti all'associazione, che va tuttavia considerato non particolarmente rilevante in quanto alcuni di questi certificatori sono attivi solo formalmente o dedicati al supporto di attività interne di soggetti o gruppi industriali, ed altri iscritti all'elenco solo da pochissimo tempo e quindi da ritenere ancora in fase di attivazione.

[25] Dati cortesemente forniti da Infocamere.

[26] Dati cortesemente forniti dal Ministero dell'Economia e delle Finanze.



	Mar 2004	Feb 2004	Gen 2004	Dic 2003	Nov 2003	Ott 2003	Set 2003	Ago 2003	Lug 2003	Giu 2003	Mag 2003	Apr 2003
Effettivi	137.552	113.429	106.470	160.869	103.503	95.569	47.368	39.423	95.912	57.262	43.677	35.861
Di Prova	76.545	60.661	59.451	90.760	60.958	55.382	28.628	18.984	57.240	37.936	30.378	23.611
TOTALE	214.097	174.090	165.921	251.629	164.461	150.951	75.996	58.407	153.152	95.198	74.055	59.472

Possiamo quindi stimare in almeno 250.000, al mese di aprile 2004, il numero di documenti informatici sottoscritti ogni mese digitalmente dai notai italiani, con una media di circa sessanta documenti per ogni notaio[27] ed un totale annuo di sottoscrizioni digitali da parte dei notai di circa 3.000.000.

Tale numero è destinato almeno a raddoppiare con l'estensione a tutti gli atti della registrazione telematica, prevista per il mese di giugno 2004.

Tali dati appaiono particolarmente significativi in un quadro in cui lo sviluppo dell'uso delle tecnologie dell'informazione, pur in rapida evoluzione, non è da considerare particolarmente avanzato. Nel 2000 (ultimo dato disponibile relativo ad un'indagine ufficiale di carattere generale su tutto il territorio nazionale) l'uso del personal computer era esteso al 29,6% della popolazione[28].

[27] Le stime sono fondate anche sull'andamento medio delle vendite immobiliari e dei mutui ipotecari degli ultimi anni, che hanno visto una media annua di circa 900.000 vendite immobiliari e 380.000 mutui ipotecari nel triennio 1999 – 2001 (dati dell'Istituto Nazionale di Statistica reperibili sul sito http://www.istat.it).

[28] Dati Istat reperibili sul sito http://www.istat.it. Secondo tale indagine nel 2000 il 29,6% delle persone di 3 anni e più (pari a 16 milioni e 400mila individui) usa il pc. L'uso di questo mezzo ripropone, seppure con diversa intensità, le classiche geografie delle disuguaglianze legate al genere, al rapporto Nord/Sud, alla condizione professionale e al livello di istruzione. In primo luogo i dati evidenziano l'esistenza di un consistente divario tra uomini e donne. Sono di più gli uomini che usano il personal computer (il 34,3% rispetto al 25,1% delle donne) ma le differenze sono molto più contenute tra i giovani fino ai 24 anni. In particolare si registra un forte vantaggio a favore delle donne tra le bambine di 3-5 anni del Nord-est (21,4% rispetto al 10,7% dei bambini della stessa ripartizione) e le persone tra i 20 e i 24 del Nord-ovest (67,2% rispetto al 60,4% dei coetanei maschi). Le differenze di genere si amplificano notevolmente dai 25 anni in poi e tale andamento è valido anche rispetto alle diverse ripartizioni geografiche. Sono i giovani ad usare di più il personal computer: tra i bambini di 6-10 anni il tasso di utilizzo è del 34,8% e supera il 50% tra gli 11 e i 24 anni. Le percentuali decrescono nelle età successive

Altro dato significativo è quello relativo all'uso di Internet o di collegamenti telematici che, sempre con riferimento al 2000, riguardava una percentuale del 18,5% della popolazione, ma è da considerare, pur in mancanza di dati ufficiali, almeno triplicato ad oggi. [29] Per quanto riguarda l'altro indicatore costituito dalla percentuale di uso della posta elettronica, esso è da considerare generalizzato tra gli utenti di Internet [30].

---

riducendosi al 27,4% tra i 45-54enni e all'1,9% tra gli ultrasessantacinquenni. Il territorio influenza notevolmente l'uso del personal computer. Al Nord la percentuale di utilizzatori è di circa il 35%, al Centro si registra un valore di poco inferiore (31,1%) mentre al Sud e nelle Isole il tasso di utilizzo del pc è decisamente più contenuto (rispettivamente 22,8% e 20,5%). Gli studenti sono la categoria di persone che ha il tasso di utilizzo del pc più elevato (68,1%) con una differenza tra uomini e donne di circa 8 punti percentuali (rispettivamente 72,4% e 64,3%). Tra gli occupati sono i dirigenti, gli imprenditori e i liberi professionisti e i direttivi, quadri e impiegati ad avere i tassi di utilizzo più elevati (63,9%), seguiti dai lavoratori in proprio e coadiuvanti (27,6%).Il titolo di studio comunque è la variabile che influenza in modo più evidente l'uso del personal computer. Il 68,1% dei laureati usa il pc rispetto all'11,1% delle persone con la licenza elementare o nessun titolo e questo divario diventa ancora più forte se si considerano le persone tra i 25 e i 44 anni (79,9% dei laureati usa il pc rispetto al 2,6% dei coetanei con la licenza elementare o nessun titolo), per poi attenuarsi leggermente nelle classi di età più avanzate. Per quel che riguarda la frequenza di utilizzo vi è da rilevare una forte concentrazione di persone che usano il pc con continuità: la quasi totalità degli utilizzatori (87,3%) vi ricorre almeno una volta alla settimana e ben il 54% lo usa tutti i giorni. Il personal computer viene utilizzato prevalentemente per 1-2 ore al giorno (24,9%) o per 2-3 ore al giorno (15,4%), mentre risulta cospicua la quota di coloro che non riescono a quantificare il tempo trascorso davanti al pc (18,5%).

[29] La fruizione di internet (18,5%) è caratterizzata da un forte divario generazionale a favore dei giovani (nella classe tra i 20-24 anni, con il 38,3%, si riscontra il valore più alto di utilizzo) e da significative differenze di genere. Se in totale lo scarto tra uomini e donne è di circa 9 punti percentuali, il fenomeno assume valori diversi in relazione all'età: tra i giovani di 20-24 anni lo scarto è di soli tre punti percentuali, mentre aumenta per le classi di età successive (tra i 55 e i 59 anni, ad esempio, gli uomini arrivano al 12,2% mentre le donne superano di poco il 3%). Il fenomeno presenta inoltre delle forti differenze legate al titolo di studio e alla condizione professionale. Sono il 51,8% i laureati che usano il web, mentre sono il 2,9% quelli in possesso della licenza elementare o nessun titolo. Anche a parità di titolo di studio permangono delle differenze tra maschi e femmine. Ad esempio tra i laureati di 25-44 anni gli uomini che usano internet sono il 72,9% rispetto al 54,2% delle laureate della stessa classe di età. Le differenze di genere però, a parità di titolo di studio, sono meno forti per i ragazzi tra gli 11 e i 13 anni (la differenza tra maschi e femmine per gli 11-13enni con la licenza media è inferiore ad un punto percentuale). Le differenze aumentano tra i 14-24enni, ma è nelle età successive che il divario tra maschi e femmine si amplifica considerevolmente (gli uomini diplomati tra i 45 e i 64 anni che usano internet sono poco meno del doppio delle coetanee con pari titolo di studio). Tra gli occupati, i dirigenti, gli imprenditori e i liberi professionisti sono i fruitori più forti (49,1%), seguiti dai direttivi, quadri e impiegati (che arrivano a circa il 40%), mentre gli operai presentano i valori più bassi. Sul versante dei non occupati si riscontra invece un cospicuo 47,6% di studenti che utilizzano internet. A parità di condizione professionale, anche in questo caso vi sono forti differenze di genere: ad esempio il 53% degli studenti usa internet rispetto al 42,4% delle studentesse e il 45% dei direttivi, quadri e impiegati al 34,9% delle donne nella stessa condizione professionale. Il divario è però meno marcato tra i dirigenti, imprenditori e liberi professionisti (50,2% rispetto al 45,8% delle femmine). Le persone che navigano su internet, come d'altronde quelle che usano il pc, lo fanno generalmente in modo assiduo. Il 31,1% degli utilizzatori si collega alla rete tutti i giorni e il 44,4% una o più volte a settimana. Tra i dirigenti, i liberi professionisti e gli imprenditori, a testimonianza della significativa penetrazione del web nel mondo del lavoro, l'uso diventa ancora più intensivo e si arriva al 41,2% che lo usa tutti i giorni e ad un altro

40% che vi ricorre una o più volte alla settimana. Internet risulta molto caratterizzato da un uso domestico: il 38% dei navigatori lo usa solo da casa e il 30,7% lo usa sia da casa che da fuori casa. Solo un quarto dei navigatori, invece, lo usa esclusivamente fuori casa.

[30] Circa due terzi dei naviganti (63,7%) ricorre allo strumento della posta elettronica. Anche in questo caso, emergono significative differenze rispetto all'età degli utilizzatori (con un picco di utilizzo del 72% tra i 25-34enni). Tra gli occupati sono i dirigenti, gli imprenditori e i liberi professionisti ad avere il tasso più elevato di utilizzo della posta elettronica (73,2%), e anche in questo caso i tassi di

Ricerche più recenti[31] rivelano il livello di sviluppo del mondo delle imprese rispetto all'utilizzazione delle tecnologie dell'informazione. Un'indagine svolta dall'Istat sulle imprese da 10 a 249 addetti misura la diffusione e l'utilizzo delle *ICT*, la presenza delle imprese sul *web* e l'impiego del commercio elettronico, acquisendo informazioni anche su motivazioni, benefici e ostacoli relativi all'utilizzo delle tecnologie informatiche e delle reti di comunicazione.

A gennaio del 2003 il 94,6% delle imprese italiane con almeno 10 addetti ha un personal computer, facendo registrare rispetto a gennaio 2002 solo un lieve aumento di 0,8 punti percentuali. In maggiore crescita sono le quote di addetti che utilizzano il pc almeno una volta alla settimana (43,8% nel 2003 e 41,8% nel 2002) e di addetti che utilizzano computer connessi ad Internet (24,3% nel 2003 e 20,9% nel 2002). In aumento anche la quota di imprese che utilizza l'e-mail (76,7%, 1,7 punti percentuali in più rispetto al 2002), la rete Internet (81,5%, 4 punti percentuali in più rispetto al 2002) e che è provvista di un sito web (49,6% nel 2003 e 47,3% nel 2002).

Le imprese utilizzano Internet soprattutto per ottenere servizi finanziari e per ricercare informazioni utili all'analisi del mercato o per fornire servizi legati a scopi pubblicitari e solo in minima parte per effettuare transazioni *on-line*. Nell'anno 2002 il 9,8% (1,9 punti percentuali in più rispetto al 2001) delle imprese ha effettuato acquisti *on-line* per un valore complessivo pari al 2,6% degli acquisti totali sia *on-line* che off-line (1,9 punti percentuali in più rispetto al 2001) e il 4,7% delle imprese ha venduto *on-line* beni e servizi (dato invariato rispetto al 2001) per un valore complessivo pari al 2,0% del fatturato totale (nel 2001 era pari al 2,5%)[32]. A gennaio del 2003 più della

---

utilizzo dei maschi sono di poco superiori a quelli delle donne (74,8% rispetto a 68%). Tra i non occupati sono invece le persone in cerca di prima occupazione ad avere i tassi di utilizzo più elevati (64,7%) seguiti dagli studenti (64%). Il titolo di studio influenza molto l'abitudine ad usare la posta elettronica: il 75,1% dei laureati che usa internet usa anche la posta elettronica rispetto al 36,1% dei naviganti con la licenza elementare o nessun titolo e la differenza si mantiene tale sia tra le persone di 25-44 anni che tra gli ultrasessantacinquenni. Anche la condizione professionale influenza molto le attività che si realizzano con internet. Il gioco e il partecipare a chat e newsgroup è praticato soprattutto dagli studenti (rispettivamente 43,7% e 36,3%). I dirigenti, gli imprenditori e i liberi professionisti usano più degli altri internet per acquisire documenti (61,9%), per utilizzare servizi (32,5%) e per acquistare e vendere attività finanziarie (7%), mentre le persone in cerca di prima o nuova occupazione sono ovviamente coloro che usano di più internet per cercare lavoro (35-42%).

[31] Il periodo di riferimento è maggio-dicembre 2003.

[32] Dal lato degli acquisti *on-line* il 9,8% delle imprese al di sopra dei 10 addetti ha effettuato nel 2002 transazioni economiche, per un valore complessivo pari al 2,6% degli acquisti totali (sia *on line* che *off-line*). Dal lato delle vendite, solo il 4,7% delle imprese al di sopra dei 10 addetti ha effettuato nello stesso anno transazioni *on-line* per un valore complessivo pari al 2,0% delle vendite totali (*on-line* e *off-line*). Le imprese dei servizi mostrano quote in valore delle transazioni *on-line* inferiori a quelle delle imprese industriali dal lato delle vendite e superiori dal lato degli acquisti: per l'industria la quota di valore degli acquisti è del 1,9% e quella delle vendite del 2,6%, mentre per i servizi le due quote sono, nell'ordine, 3,3% e 1,2%. Sia la numerosità relativa delle imprese che effettuano acquisti o vendite *on-line* che la percentuale del valore degli scambi effettuati *on-line* tendono ad aumentare fortemente con la dimensione delle imprese. Tra quelle con 250 addetti e oltre le imprese che effettuano acquisti *on-line* sono il 22,3% e la quota dei valori acquistati è pari al 4,3%. Nel caso delle vendite le due quote sono rispettivamente pari al 21,9% e al 3,1%. *Internet* è la rete più frequentemente utilizzata dalle imprese per effettuare sia acquisti (90,4% delle imprese che acquistano *on-line*) sia vendite (68,7% delle imprese che vendono *on-line*). Tuttavia il valore degli scambi effettuati via *Edi* è nettamente più alto di quello realizzato tramite *Internet*. Infatti mediante la prima viene effettuato il 72,0% del valore degli acquisti *on-line* e l'82,9% del valore delle vendite *on-line*. Tra i benefici derivanti dall'utilizzo di *Internet* per effettuare acquisti, le imprese attive nel 2002 nel commercio elettronico via *Internet* hanno indicato con più elevata frequenza la maggiore velocità dei processi (79,1%) e la possibilità di scegliere tra un'offerta

metà delle imprese ha utilizzato servizi bancari informativi offerti sulla rete relativi ai conti correnti e il 44,3% delle imprese si è avvalso dei servizi di natura dispositiva (pagamenti, incassi, bonifici, ecc.)[33]; rispetto al 2002 tali quote hanno registrato incrementi rispettivamente di circa 8 e 9 punti percentuali.

Infine, circa il 66,0% delle imprese utilizza la rete anche per usufruire dei servizi informativi offerti sui siti web dalla Pubblica Amministrazione mentre ben il 52,1% delle imprese utilizza i servizi di pagamento *on-line* offerti dalla P.A. (indicando grandi passi in avanti rispetto all'11,8% registrato nel 2002).[34]

---

più numerosa (64,9%), seguiti dalla riduzione dei prezzi (56,7%), dei costi (55%) e delle rimanenze (18,9%). Pur con qualche oscillazione intorno alle frequenze medie di risposta, le stesse indicazioni emergono dai dati disaggregati per macrosettore di attività economica, per classi di addetti e per ripartizioni geografiche Con riferimento agli ostacoli ad effettuare acquisti via *Internet* le imprese attive nel commercio elettronico via *Internet* considerano più importanti il limitato numero di fornitori in grado di ricevere ordini *on-line* (71,1%), la scarsa sicurezza dei pagamenti (65,6%), la difficile adattabilità delle proprie attività ad uno scambio elettronico (63,7%), l'incertezza del quadro legale di riferimento (60,8 %). Seguono, con percentuali tra il 39,2% ed il 29,7%, gli ostacoli inerenti problemi logistici, la difficile integrazione con la contabilità aziendale, gli elevati costi di consegna e l'utilizzo delle lingue straniere. Tra le imprese che praticano il commercio elettronico via *Internet*, i pagamenti eseguiti con lo stesso mezzo sono effettuati da significative quote di imprese, soprattutto dal lato degli acquisti. Nel 2002 poco meno del 42,0% delle imprese con acquisti via *Internet* ha utilizzato la rete anche per i correlati pagamenti, mentre dal lato delle vendite l'analoga quota è stata del 15,0%. Molto più basse risultano le due incidenze percentuali dei pagamenti via *Internet* sul totale dei valori acquistati o venduti tramite rete: nel primo caso il rapporto è pari al 2,8%, mentre nel secondo è stato leggermente inferiore, pari al 2,0%.Nel caso degli acquisti i pagamenti via *Internet* sono più frequenti tra le imprese industriali (43,8%); meno tra quelle dei servizi (40,4%). La diffusione dei pagamenti via *Internet* per acquisti in rete tra le imprese appartenenti alle diverse classi di addetti e tra quelle localizzate nelle varie ripartizioni geografiche risulta piuttosto omogenea, con quote comunque vicine alla media.

[33] Nei rapporti con le banche circa il 56,5% delle imprese utilizza i servizi informativi sul conto corrente (estratto conto, saldo, insoluti, ecc.), il 44,3% i servizi dispositivi (pagamenti, incassi, bonifici, ecc.) ed il 31,2% i servizi relativi allo scambio di flussi elettronici per operazioni bancarie e commerciali (*corporate banking* interbancario). Rapportando gli stessi valori al totale delle imprese con accesso ad *Internet*, le percentuali raggiungono rispettivamente il 69,3%, il 54,4% e il 38,2%. Nelle prime due tipologie di servizi bancari telematici, le imprese appartenenti al macrosettore industria, alle classi di addetti intermedie (da 50 a 249 addetti) e a quelle localizzate nelle ripartizioni settentrionali presentano quote di utilizzo superiori ai valori medi. Anche in questi segmenti i servizi meno utilizzati sono quelli relativi ai finanziamenti (aperture di credito e mutui *on-line*) con il 2,1% e agli acquisti e vendite di titoli *on-line* (investimenti finanziari) con l'1,2%. A livello settoriale è interessante notare come per i tre servizi più utilizzati i settori più attivi sono, nell'industria, quelli della produzione di energia, della fabbricazione di pasta e carta e quello della fabbricazione di prodotti chimici; nei servizi quelli dell'informatica e del commercio all'ingrosso. Rispetto all'anno precedente le percentuali relative alla somma delle quote di uso attivato e pianificato dei primi due servizi (informativi, di incasso e pagamento) sono aumentate in entrambi i casi di circa 5 punti percentuali (da 55,5% a 61,7% il primo e da 45,2% a 50,6% il secondo).

[34]La rete viene utilizzata dalle imprese anche per accedere ai servizi offerti dai siti *web* delle amministrazioni pubbliche. In generale il ricorso ai servizi pubblici *on-line* è più diffuso tra le imprese di maggiori dimensioni, mentre a livello territoriale le quote di diffusione rilevate nelle singole ripartizioni variano sensibilmente secondo il servizio utilizzato. Nelle regioni settentrionali sono relativamente più diffusi rispetto alle altre ripartizioni i servizi di informazione e quelli inerenti la ricezione e l'invio di moduli. Nelle regioni meridionali vi è un utilizzo relativamente più frequente dei servizi che offrono informazioni *on-line* sulle opportunità di partecipazione ad operazioni di *eprocurement*. A livello nazionale il servizio più diffuso è quello volto ad ottenere informazioni (66,2%) con punte fino all'91,0% nel settore della produzione di energia e dell'89,8% in quello dell'informatica. Tra i servizi offerti *on-line* dalla PA, che richiedono una partecipazione delle imprese più attiva rispetto alla semplice ricerca di informazioni e allo scambio di moduli, il più utilizzato è quello relativo all'accesso alle pratiche amministrative come richieste di concessioni, autorizzazioni, licenze, brevetti (19,8%), seguito da quello volto all'assolvimento delle procedure amministrative (18,4%), dai pagamenti *on-line* verso la PA

L'osservazione di carattere generale che si può ricavare è che le imprese sono ancora in massima parte nella fase iniziale dell'uso dei servizi in rete, relativa all'acquisizione ed alla fornitura di informazioni reperibili con i mezzi tradizionali, e solo in minima parte, fatta eccezione per il settore bancario che gode di un maggiore sviluppo, utilizzano tali servizi per vere e proprie transazioni commerciali *on-line*.

Il complesso dei dati esposti, rapportato allo sviluppo informatico del sistema paese, rende evidente la posizione di avanguardia del notariato nel processo di informatizzazione dell'economia, e dei servizi pubblici in particolare.

In particolare l'assunzione del ruolo di Autorità di Certificazione segna uno dei passaggi fondamentali dell'assunzione di un ruolo sempre più attivo del notariato in tali processi, nell'ambito di un'evoluzione che data da oltre un decennio[35], e lascia prevedere ulteriori sviluppi.

Nelle pagine che seguiranno osserveremo quali sviluppi di interesse notarile sono previsti dai progetti governativi.

3. I futuri sviluppi della informatizzazione della Pubblica Amministrazione italiana.

I più recenti progetti evolutivi dell'informatica nella Pubblica Amministrazione sono contenuti nel piano triennale per l'eGovernment 2004-2006[36]. Il piano nasce in concomitanza con la piena attuazione del processo di riorganizzazione dell'informatica pubblica, innestato dalla nomina del Ministro per l'innovazione e le tecnologie, e dalla creazione del relativo Dipartimento[37]. Il piano triennale elaborato raccoglie, consolida e traduce in programmi operativi gli indirizzi strategici elaborati e diffusi negli ultimi due anni dal Ministro per l'innovazione e le tecnologie. Tra questi, in primo luogo, gli "obiettivi di legislatura", illustrati nel documento approvato il 13 febbraio 2002 dal Comitato dei ministri per la Società dell'informazione. Tali obiettivi, finalizzati al miglioramento dei servizi verso cittadini e imprese, all'efficienza interna, alla valorizzazione delle risorse umane, alla trasparenza e alla verifica della soddisfazione degli utenti nonché alla qualità dei servizi, ed i cui risultati finali sono programmati per il 2005, sono:

Servizi online ai cittadini e alle imprese

1. Tutti i servizi 'prioritari' disponibili *on-line*

(13,3%) ed infine da quello volto a far partecipare le imprese alle aste telematiche *on-line* (*e-procurement*) con il 6,7% delle imprese.

[35] Sulle precedenti realizzazioni del Consiglio Nazionale del Notariato in tale settore, sulla creazione della società d'informatica del notariato italiano (Notartel spa) e sui servizi informatici e telematici forniti ai notai a supporto dell'attività professionale cfr. la relazione di F. SALERNO CARDILLO al *XXIII Congresso del Notariato Latino*, reperibile nei relativi atti, Milano, 2001, pag. 533 ss..

[36] Il piano può essere integralmente consultato all'indirizzo http://www.cnipa.gov.it.

[37] L'articolo 26 della legge 289 del 2002 ha, inoltre, attribuito nuovi poteri al Ministro per l'innovazione e le tecnologie, quali l'approvazione dei piani per l'informatica delle varie amministrazioni, di concerto con il Ministro dell'economia e delle finanze, la valutazione dei progetti di valenza strategica, l'individuazione ed il coordinamento dei "progetti intersettoriali", che coinvolgono più amministrazioni, la valutazione del corretto utilizzo delle risorse. In questo quadro si valorizzano l'impulso ed il coordinamento delle attività volte alla piena informatizzazione.

2. 30 milioni di Carte di identità elettroniche e Carte nazionali dei servizi distribuite[38];

3. 1 milione di firme digitali diffuse entro il 2003[39];

Efficienza interna della Pubblica Amministrazione

4. 50% della spesa per beni e servizi tramite eProcurement[40]

5. Tutta la posta interna alla Pubblica Amministrazione via e-mail[41], con utilizzazione massiva della posta elettronica certificata[42] e del protocollo informatico[43] (il che consente un risparmio notevole in costi dei servizi postali ed in rapidità di comunicazione);

6. Tutti gli impegni e mandati di pagamento gestiti *on-line*

Valorizzazione delle risorse umane

7. Alfabetizzazione certificata dei dipendenti pubblici;

8. 1/3 della formazione erogata via eLearning[44];

Trasparenza

9. 2/3 degli uffici della Pubblica Amministrazione con accesso *on-line* all'iter delle pratiche da parte dei cittadini;

---

[38] La carta d'identità elettronica (CIE) e la carta nazionale dei servizi (CNS) costituiscono iniziative congiunte del Ministro per l'Innovazione e le Tecnologie, del Ministero dell'Interno e del Ministero della Salute. L'Italia è il primo Paese europeo ad avere introdotto una Carta d'Identità Elettronica, basata su microprocessore. La CIE permette inoltre il riconoscimento del cittadino nell'uso dei servizi in Rete della Pubblica Amministrazione sul territorio nazionale. È stata avviata una seconda fase di sperimentazione nella quale saranno distribuite 1,5 milioni di carte in 56 Comuni. Poiché la distribuzione richiederà alcuni anni è stata introdotta la Carta Nazionale dei Servizi la cui diffusione sarà invece molto rapida. La CNS, con lo stesso standard della CIE, permetterà soltanto l'accesso ai servizi di *e-Government*.

[39] Come si è visto, si tratta di un obiettivo già superato in misura superiore al 50% del risultato programmato.

[40] Si tratta di un sistema che consente l'approvvigionamento della Pubblica Amministrazione attraverso gare telematiche; è un'iniziativa del Ministro per l'Innovazione e le Tecnologie e del Ministero dell'Economia e delle Finanze. Con gli acquisti in Rete da parte delle pubbliche amministrazioni si realizzano obiettivi di efficienza, velocità e trasparenza. Nel 2002 il risparmio potenziale è stato di 2,3 miliardi di euro e le previsioni per il 2003 (non sono ancora disponibili i dati definitivi) sono di 3,4 miliardi di euro.

[41] Ogni lettera, oggi, costa alla P.A. circa 20 euro contro i 2 euro di un messaggio di posta elettronica. La diffusione di PC nelle pubbliche amministrazioni statali ha raggiunto circa il 90% dei dipendenti. È stata emanata una Direttiva del Ministro per l'Innovazione e le Tecnologie di concerto con il Dipartimento della Funzione Pubblica che getta le basi affinché entro la fine di questa legislatura tutte le comunicazioni interne della P.A. avvengano tramite posta elettronica. Con l'uso della firma digitale e della posta certificata i dipendenti pubblici avranno la certezza dell'autenticità del documento e del suo avvenuto ricevimento da parte dei destinatari.

[42] E' in corso di emanazione un provvedimento normativo relativo al pieno riconoscimento della posta elettronica certificata come strumento legale di trasmissione riconosciuto ed alternativo al servizio postale tradizionale.

[43] Il protocollo informatico, utilizzato già dal 25% degli uffici pubblici, permette lo scambio in formato digitale della documentazione fra pubbliche amministrazioni con significativi incrementi di efficienza, e i successivi stati del trattamento, della classificazione, e del recupero delle informazioni. Dal 1° gennaio 2004 le pratiche presentate agli uffici pubblici iniziano ad essere gestite in Rete, un primo passo per permettere a cittadini e imprese di conoscere in tempo reale stato e iter dei procedimenti di loro interesse.

[44] E'in corso di emanazione la "Direttiva e Linee Guida sull'e-learning per le pubbliche amministrazioni" cui seguirà un Vademecum e un'attività di informazione e formazione. L'obiettivo è promuovere l'utilizzo dell'e-learning (apprendimento a distanza) di qualità nella P.A. per elevare le professionalità del personale pubblico, ma anche fornire regole chiare ad un mercato in espansione per favorirne lo sviluppo.

Qualità

10. Tutti gli uffici che erogano servizi dotati di un sistema di soddisfazione dell'utente.

Vi sono poi altri obiettivi, inizialmente non previsti come prioritari, ma la cui importanza si è rivelata fondamentale con lo sviluppo delle attività come quelli relativi alla sicurezza informatica[45] e quelli relativi all'utilizzazione del software Open-Source nella Pubblica Amministrazione[46].

Tra questi obiettivi generali, che sono in ogni caso un indicatore efficiente delle tendenze evolutive del sistema, sono stati individuati obiettivi particolari di singoli settori di interesse. Alcuni di questi sono di particolare rilevanza per il notariato in quanto possono costituire occasioni di miglioramento funzionale dei servizi resi dalla categoria o, anche, di ampliamento delle attività e delle competenze.

Ci riferiamo in particolare alle attività del Ministero dell'Economia e delle Finanze, per quanto attiene i settori dell'imposizione indiretta e l'imposizione sugli immobili in genere, e del Ministero della Giustizia, per le attività di diretto interesse notarile.

Il Ministero dell'Economia e delle Finanze ha maturato una notevole esperienza nel settore dei servizi *on-line* delle agenzie fiscali ed ha già registrato risultati di rilievo e riconoscimenti internazionali. Le nuove proposte riguardano la dichiarazione di successione *on-line*, la verifica dello stato delle pratiche di sgravio e rimborsi, la consultazione della posizione fiscale, la presentazione telematica di istanze e richieste di vario genere (interpello, rimborsi, autotutela, sgravi), la registrazione di atti giudiziari, il processo tributario *on-line*.

In particolare, per quanto riguarda l'area tributaria più propriamente detta, gestita dall'Agenzia delle Entrate, il progetto Servizi prioritari disponibili *on-line*, che si integra con quello del Servizio telematico delle dichiarazioni e degli atti, in base al quale è già possibile da anni presentare un notevole numero di documenti fiscali in modalità telematica, è focalizzato sia sul potenziamento dei servizi già attivati sia sull'erogazione ed estensione di nuovi:

- dichiarazione di successione: possibilità, per il contribuente, anche avvalendosi di intermediario, di presentare via Internet la dichiarazione di successione tramite apposita applicazione web per la compilazione guidata; si tratta di un servizio di diretto interesse del notariato, essendo la dichiarazione di successione presupposto per la libera trasferibilità degli immobili secondo la legislazione italiana, e tradizionale settore di intervento dell'attività libero professionale del notaio;

- registrazione atti giudiziari: registrazione on-line degli atti giudiziari; anche questo settore, essendo ormai attuata la riforma che prevede la delega al notaio delle vendite forzate immobiliari e mobiliari, è di immediato interesse del notariato, in quanto

[45] Si tratta di un'iniziativa del Ministro per l'Innovazione e le Tecnologie e del Ministero delle Comunicazioni che ha individuato due aree di intervento prioritarie: la prima riguarda l'istituzione di un nucleo di competenza (denominato CERT) per il monitoraggio, la prevenzione e la gestione degli incidenti informatici a supporto delle Amministrazioni; la seconda un piano di formazione in materia di sicurezza informatica nella P.A.

[46] il Ministro per l'Innovazione e le Tecnologie ha emanato una direttiva che fornisce le regole per la valutazione di scelte informatiche che tengano in considerazione anche i software *Open Source*, cioè a "codice sorgente aperto". Questi software permettono a chiunque abbia le competenze tecniche adeguate di apportarvi modifiche utili per le proprie attività, agevolandone il riuso nell'ambito delle varie amministrazioni pubbliche.

interessa le modalità operative di tale attività, ed è funzionale alla soddisfazione dell'esigenza di maggiore efficienza e velocità che è stata alla base dell'affidamento di tali funzioni ai notai;

- posizione fiscale: consultazione della posizione fiscale dei contribuenti da parte dei diretti interessati o dei soggetti autorizzati; anche in questo caso, la possibilità di consultazione da parte del notaio può contribuire ad evitare le problematiche relative alla sussistenza di privilegi immobiliari per ragioni di carattere fiscale;.

- stato delle pratiche amministrative: possibilità per il contribuente di avere informazioni *on-line* sullo stato di avanzamento delle pratiche relative a provvedimenti di sgravio e a rimborsi d'imposta;

- presentazione di istanze e richieste generiche: presentazione in maniera telematica di istanze e richieste di vario genere (interpello, rimborsi, autotutela, sgravi, ecc.).

Altro progetto di grande rilevanza per il Notariato è quello che prevede la diffusione massiva della firma digitale tra i dipendenti dell'amministrazione finanziaria con potere di firma (responsabile di uffici centrali e periferici, direttori centrali, regionali e loro delegati). All'attuazione di tale progetto sarà possibile dialogare, in modo perfettamente imputabile sia all'interno dell'amministrazione, sia nei confronti dell'utente esterno. E' di tutta evidenza l'importanza del progetto per una completa attuazione di processi basati sul documento informatico.

Per le attività ricollegabili alla gestione del catasto e delle pubblicità immobiliare, di competenza all'interno del Ministero dell'Agenzia del Territorio, e di diretto interesse del Notariato, l'intervento di maggior rilievo è costituito dal progetto *Dematerializzazione*. Esso è finalizzato a fornire i servizi di base per la piena digitalizzazione dei flussi informativi interni ed esterni. Gli interventi riguardano l'uso della firma digitale e la posta certificata, l'archiviazione degli atti con firma digitale e la possibilità di accettazione e numerazione delle formalità ipotecarie trasmesse per via telematica. La realizzazione di tale progetto comporta interventi di rilievo sul sistema attuativo della pubblicità immobiliare, che richiederanno, con ogni probabilità, interventi normativi volti a modificare ed integrare il codice civile. Il notariato è coinvolto attivamente nella realizzazione di tale progetto, che costituisce, oltre che un modello di gestione documentale totalmente telematizzata di un pubblico registro, un'ipotesi applicativa di straordinaria complessità dei sistemi di conservazione del documento informatico e della sua rilevanza giuridica.

Gli ulteriori sviluppi dei servizi *on-line* sono inseriti nel progetto *Servizi telematici*. Le attuali linee di azione sono l'estensione dei servizi ad altre tipologie di utenti (persone fisiche) con l'incremento dell'offerta di servizi (visure ipocatastali, statistiche di mercato, fornitura di dati in formato elaborabile ecc.), l'incremento delle tipologie di documenti (documenti di aggiornamento catastale, atti notarili soggetti a registrazione, atti giudiziari e dichiarazioni di successione) trasmessi in via telematica e la trasmissione telematica ai comuni dei dati delle dichiarazioni ICI (Imposta Comunale sugli Immobili). Al riguardo, nel corso del 2003, è stata condotta la sperimentazione dell'invio telematico ai comuni dei dati delle dichiarazioni ICI, desunti dagli atti immobiliari registrati in via telematica, nell'ambito del protocollo di intesa stipulato tra l'Agenzia del Territorio, l'Anci ed il Consiglio nazionale del Notariato. Nel corso di un triennio si prevede di estendere il servizio a tutti i comuni ed a tutte le tipologie di trasferimenti immobiliari trasmessi in via telematica, ivi compresi gli atti giudiziari e le successioni, consentendo in tal modo di eliminare l'obbligo di presentazione delle

dichiarazioni di variazione ICI (Imposta Comunale sugli Immobili), oggi a carico dei cittadini. Il successo delle iniziative è vincolato a interventi di revisione normativa, alla cui predisposizione partecipa con proprie proposte il Consiglio Nazionale del Notariato.

Nel settore di attività del Ministero della Giustizia si segnala il Processo civile telematico, che renderà disponibili via web il deposito di atti, la consultazione dello stato delle cause ed il fascicolo elettronico, la trasmissione di comunicazioni, notifiche e copie di atti dagli uffici giudiziari ai soggetti coinvolti, e che è di diretto interesse del notariato in relazione al sistema delle aste immobiliari derivanti dal processo esecutivo sugli immobili, che vengono svolte, per la più gran parte dei casi, dai notai. È programmato anche il sistema di pubblicità per le aste mobiliari e immobiliari elettroniche per migliorare l'efficacia e la trasparenza delle vendite giudiziarie. Esso garantirà una più agevole partecipazione all'asta per i cittadini. Sempre in tale ambito va segnalato il progetto per *l'archiviazione documentale* che prevede la realizzazione di un prototipo di sistema per la classificazione e archiviazione dei fascicoli processuali chiusi (e degli atti in esso contenuti), da sperimentare presso sedi campione, con l'intento di disporre di un prodotto standard specializzato nella gestione degli archivi di "deposito" da diffondere successivamente presso gli altri uffici giudiziari.

CAPITOLO II

LA FIRMA DIGITALE

SOMMARIO. 1. L'adozione della firma digitale in Italia; 1.1. Thick laws e thin laws; 1.2. Il sistema a chiavi asimmetriche; 2. L'equiparazione tra firma digitale ed autografa; 2.1. Atti sottoscrivibili; 2.2. La provenienza del documento firmato; 2.2.1. I rischi di origine umana: le Autorità di Certificazione; 2.3. Solennità della sottoscrizione; 2.4. Accessibilità; 3. Il regime probatorio; 4. La delega de facto; 5. La morte del titolare; 6.1. La Direttiva 93/1999; 6.2. Il D.Lgs. 10/2002; 7. La firma digitale affonda?

1. L'adozione della firma digitale in Italia

Nella seconda metà degli anni Novanta, il legislatore italiano fu uno tra i primi nel mondo a disciplinare la firma digitale e, più in generale, la documentazione elettronica. La legislazione adottata nel 1997 [47] equipara il documento provvisto di firma digitale [48] a quello in forma scritta tradizionale. Erano trascorsi appena due anni dall'emanazione della prima storica legge in materia di firma digitale, quella dello Stato americano dello Utah.

Tale solerzia, in verità alquanto inconsueta, da parte del legislatore italiano nel disciplinare questa nuova tecnologia ha un'origine storico/politica ben identificabile. Con alcune brillanti ma circoscritte eccezioni, la Pubblica Amministrazione italiana non ha una spiccata tradizione di qualificazione ed efficienza. Se l'Italia è Paese dalla storia antica, lo Stato italiano è da parte sua una realtà relativamente giovane, non avendo ancora raggiunto i 150 anni, ed ha vissuto in una fase determinante della sua evoluzione il trauma dell'esperienza fascista. Nella seconda metà del ventesimo secolo, inoltre, la politica italiana ha spesso guardato alla Pubblica Amministrazione come ad un serbatoio di posti di lavoro, strumento di stabilizzazione sociale e consenso. Un tale approccio penalizzava evidentemente l'efficienza complessiva dell'insieme, creando un divario sempre meno sopportabile nei confronti dei principali *partners* europei e mondiali. In questo contesto, l'informatizzazione della Pubblica Amministrazione assumeva i contorni di un'occasione storica per realizzare un repentino balzo in avanti, di un virtuoso pretesto per liberarsi finalmente di modelli organizzativi, decisionali e culturali ormai superati ed indifendibili, ma ciò nondimeno ben radicati e difficili da disinnescare.

[47] Decreto del Presidente della Repubblica 10 novembre 1997, numero 513 (Gazzetta Ufficiale della Repubblica Italiana numero 60 del 13 marzo 1998).

[48] Le espressioni firma elettronica e firma digitale hanno un impiego ormai praticamente stabilizzato, che si ritrova pressoché costante nei più recenti testi normativi in materia. Firma elettronica è qualunque metodo di autenticazione di un file o di altri dati elettronici. Si riserva invece l'espressione firma digitale per quella particolare firma elettronica (il rapporto, quindi, è di *genus ad speciem*) che garantisce in termini obiettivi l'identificazione del soggetto da cui promana la firma e l'intangibilità del materiale firmato. La maggior parte delle fonti incorpora nella definizione di firma digitale l'impiego della tecnologia a chiavi asimmetriche e l'intervento di un soggetto terzo in funzione di certificazione (la cosiddetta Certification Authority, o CA); talvolta invece tali riferimenti mancano (è il caso della definizione ISO), ritenendosi che il ricorso al sistema articolato su chiavi asimmetriche e Certification Authority (detto nel complesso PKI, Public Key Infrastructure) non corrisponda ad una necessità concettuale ma solo allo stato dell'arte corrente.

Tale contesto politico contribuisce a spiegare il ruolo che il notariato italiano si è trovato a svolgere, anch'esso caratterizzato, a cavallo tra gli anni Novanta ed il principio del nuovo secolo, da una fuga in avanti in campo informatico che è talora apparsa eccessiva se non francamente imprudente. La spinta verso un'informatizzazione (per così dire) a tutti i costi in più di un occasione ha in effetti rischiato di far passare in secondo piano le esigenze di certezza ed affidabilità (anche nel tempo) della documentazione destinata ad affluire ai Pubblici Registri: ma qui il notariato italiano, obbedendo al suo DNA, ha svolto con energia la sua naturale funzione di richiamo e contrappeso. Richiamo e contrappeso che mai però ha potuto implicare un rallentamento nell'introduzione delle nuove tecnologie: questo esito sarebbe stato percepito, sul piano dell'immagine di categoria, quale arroccamento da parte del notariato a difesa di modelli operativi superati, in danno delle prospettive di sviluppo ed evoluzione. Non mancavano d'altronde, come sempre ed ovunque, avversari in mala fede, pronti a dipingere il notariato come una zavorra di cui liberarsi, in tutto od in parte, nell'interesse del rapido progresso del Paese. Ciò ha fatto sì che il notariato italiano abbia scelto di concepire, creare e porre in funzione infrastrutture proprie di cui esso stesso ha dettato standard più stringenti di quelli correnti, affinché fornissero i servizi che il momento richiedeva, garantendo però nel contempo livelli di sicurezza ed affidabilità della documentazione non inferiori a quelli tipici del mondo cartaceo. Ormai tutto questo è storia: come in altra parte di questa relazione si illustrerà, la Rete Unitaria del Notariato è in servizio da tempo, e consente ai notai di collegarsi a qualunque Pubblico Registro del Paese; tutti gli atti italiani che abbiano ad oggetto immobili o società (e quindi, il nucleo fondamentale dell'attività notarile) vengono ormai prodotti anche in forma digitale per la trasmissione alla Pubblica Amministrazione, avvalendosi dei sistemi di firma digitale rilasciati dall'Autorità di Certificazione del Notariato, e che opera esclusivamente per i notai.

Una sottile vena d'ironia può rintracciarsi nel fatto che il notariato italiano, a dispetto di quanti lo dipingevano, per loro interesse, come un'istituzione del passato, d'ostacolo al progresso, ha finito col tagliare per primo il traguardo dell'integrale digitalizzazione. Nella primavera 2004, quando queste note vengono licenziate, i Registri delle Imprese italiani ricevono dai notai documenti in forma esclusivamente digitale mentre, paradossalmente, ancora fanno ampio ricorso alla carta gli specialisti che si occupano di trasmettere i bilanci delle società, operazione certamente meno critica sul piano giuridico e che presenta minori problemi di informatizzazione. Allo stesso modo, tutti gli atti immobiliari sono trasmessi in forma digitale dai notai, ma la gestione dei Registri Immobiliari deve ancora fare parziale affidamento sulla carta, in quanto l'Avvocatura e il Potere Giudiziario, che pure trattano documentazione destinata alla pubblicità immobiliare (sequestri, sentenze …), non sono ancora pronti alla loro gestione in forma elettronica.

1.1. Thick laws e thin laws

Le legislazioni in materia di firma elettronica sono per lo più ricondotte a due famiglie principali: le *thick laws* e le *thin laws*. Appartengono al primo filone le leggi che hanno compiuto una scelta tecnologica precisa, individuando e dettagliando modalità ed infrastrutture per la produzione delle firme ed attribuendo loro uno status giuridico preciso. *Thin laws* sono invece dette le leggi che hanno privilegiato una nozione più vaga di firma elettronica, che evita la cristallizzazione delle tecnologie esistenti stimolando ricerca e sviluppo di soluzioni nuove, tra cui i privati possono

scegliere il prodotto più confacente alle loro esigenze: è il cosiddetto approccio *technology-neutral*. In questo senso si è indirizzato soprattutto l'Electronic Signatures Act adottato nel 2000 dal Congresso degli Stati Uniti d'America.

La legislazione italiana del 1997, poi rivista a più riprese anche per armonizzarla alle prescrizioni dell'Unione Europea [49], appartiene a pieno titolo al filone delle *thick laws*. Compiva una scelta tecnologica precisa: l'infrastruttura di firme a chiavi asimmetriche. Attribuiva conseguenze giuridiche precise: la piena equiparazione alla forma scritta [50].

1.2. Il sistema a chiavi asimmetriche

La tecnologia a chiavi asimmetriche è una tecnica crittografica, individuata una prima volta in linea teorica da studiosi britannici, indipendentemente sviluppata negli USA negli anni Settanta ad opera di Diffie ed Hellman, e portata poi a maturità da Rivest, Shamir ed Adleman. Per comprendere il nesso che lega la crittografia asimmetrica alla sottoscrizione digitale converrà prendere le mosse dalla più tradizionale crittografia a chiavi simmetriche.

I sistemi di crittografia simmetrici sono ben noti a tutti fin dai banchi delle scuole elementari. Un esempio può essere il "sistema" che utilizza come chiave la sostituzione di ogni lettera con quella che immediatamente la precede nell'ordine alfabetico: ad esempio "Ibm" diviene "Hal". Ovviamente è possibile creare codici infinitamente più raffinati, come nel caso del sistema tedesco Enigma, impiegato durante la Seconda Guerra Mondiale, ma una caratteristica resta costante: chi possiede la chiave per decriptare un messaggio può creare a sua volta un messaggio nello stesso codice.

Il sistema a chiavi simmetriche presenta tuttavia svantaggi considerevoli.

In primo luogo, essendo unica la chiave, sia per la codifica che per la decodifica, è essenziale, per ragioni di sicurezza, che essa venga mantenuta segreta da entrambi i corrispondenti, perché il successo del metodo dipende appunto dalla segretezza della chiave. Sempre per esigenze di segretezza, inoltre, le chiavi non potranno essere trasmesse attraverso la rete telematica, determinando così un maggiore impegno di tempo e maggiori costi per la trasmissione a tutti gli interessati.

In secondo luogo la chiave potrà essere utilizzata esclusivamente per lo scambio di messaggi reciproci tra una sola coppia di utenti: così A potrà utilizzare la chiave x per inviare messaggi a B e B potrà fare lo stesso se vorrà inviare messaggi ad A. Ma se A vuole comunicare con C, dovrà concordare con quest'ultimo una chiave diversa, y. Quindi ogni utente dovrà munirsi di tante chiavi quante sono le persone con le quali intrattiene rapporti giuridici.

In terzo luogo la condivisione della chiave a coppie di utenti non consente la certezza dell'autenticità del messaggio inviato: uno dei due utenti potrebbe anche inviare a se stesso un documento attribuendolo all'altro possessore della chiave senza che sia possibile identificare l'autore del documento. Con il sistema di cifratura a chiavi asimmetriche, invece, gli inconvenienti sopra esposti vengono superati, anche se, va

[49] Oggi Testo Unico numero 445 del 28 dicembre 2000, successivamente più volte modificato: il testo sempre aggiornato è reperibile sul sito http://www.notarlex.it, gestito congiuntamente dalla Zecca dello Stato (editrice della Gazzetta Ufficiale) e dal Notariato italiano.

[50] La disposizione è oggi trasfusa nell'articolo 10 del TU 445/2000 appena citato.

ammesso, al prezzo di un considerevole appesantimento sul fronte computazionale, che ha spronato i ricercatori verso l'utilizzo, ogniqualvolta possibile, di tecnologie miste [51].

Nei sistemi a chiavi asimmetriche il software produce due chiavi, dette rispettivamente "chiave pubblica" e "chiave segreta": il perno dell'intero sistema consiste nel fatto che le due chiavi sono ben distinte ed è matematicamente impossibile ricavare l'una dall'altra [52].

Un file criptato con la chiave pubblica può essere letto soltanto se si possiede la relativa chiave segreta. La chiave segreta deve essere accuratamente custodita, quella pubblica può, ed anzi in un certo senso deve, essere diffusa il più possibile, senza alcuna precauzione [53].

---

[51] In primis il sistema SSL, su cui infra, nota 63.

[52] Le tecnologie a chiavi asimmetriche si basano principalmente sulle *one way functions*, o funzioni matematiche non reversibili, la più comune delle quali è il procedimento di fattorizzazione, ossia la scomposizione di un numero in numeri primi. Se è ovvio che 21 = 3 x 7, è meno elementare scoprire che 92648497 = 12157 x 7621 (che sono entrambi numeri primi), ma soprattutto si deve andare a tentativi, giacché non esiste un procedimento matematico che consenta di operare direttamente la fattorizzazione; l'operazione inversa, la moltiplicazione 12157 x 7621, viene invece compiuta in una frazione di secondo dalla più economica delle calcolatrici tascabili ad otto cifre. Quando i numeri sono di decine o centinaia di cifre, come quelli impiegati in crittografia, la scomposizione diviene un'impresa titanica; il percorso inverso, invece, resta una banale moltiplicazione, solo un po' più lunga (sempre nell'ambito dei decimi di secondo, anche per il più economico dei computers). E' sviluppando questa asimmetria matematica che si ottengono sistemi in cui l'utente è posto in grado di compiere un'operazione (verificare una firma) ma non quella inversa (generare la firma stessa); si veda infra nel testo. Per essere più precisi, però, dal punto di vista puramente matematico, ricostruire il fattore ignoto partendo da quello noto (la chiave privata partendo da quella pubblica) non costituisce un'assoluta impossibilità, bensì una (sia pure enorme) difficoltà di calcolo. I ragguagli forniti al proposito dai produttori, che invariabilmente misurano il tempo occorrente per violare i loro sistemi in settimane, mesi ed anni di lavoro di un supercomputer, si riferiscono ai cosiddetti *brutal attacks*, attacchi "stupidi", portati cioè provando in sequenza tutte le combinazioni possibili. E' ben vero che è molto improbabile che possa essere scoperto un metodo diretto di calcolo, atteso che la fattorizzazione è stata studiata sul piano teorico, senza successo, da alcuni dei più brillanti matematici degli ultimi secoli; esistono però tecniche crittografiche che possono semplificare il compito. Se ad esempio si hanno a disposizione molti documenti sottoscritti con la medesima chiave, l'analista può valersi di una ricca base di dati su cui operare. Alcuni affermano persino che si possano ricavare dati utili misurando il tempo che i computers impiegano per le operazioni di firma. E' quindi certo che i migliori laboratori, come quelli dell'americana NSA, possono tentare qualcosa (*cosa* è ovviamente un segreto ben custodito), ma occorre essere realisti: chi fosse interessato a violare una chiave di firma, troverà in genere assai più semplice ed economico corrompere un collaboratore, od intercettare da un ambiente vicino gli impulsi elettromagnetici emessi dalla tastiera, onde scoprire il PIN della *smart card* prima di procedere alla sua sottrazione: avvalersi, insomma, delle "normali" tecniche di spionaggio industriale. Anche determinati tipi di virus possono essere utilizzati a tal fine: nell'estate 2003, ad esempio, si diffuse su Internet il virus *BugBear*, le cui caratteristiche consentono al pirata di assumere il controllo del computer dell'utente del sistema di firma digitale e, col concorso di alcune circostanze a lui favorevoli, di apporre ineccepibili firme digitali all'insaputa del titolare del sistema.

[53] Se X desidera ricevere messaggi criptati da Y, potrà inviargli senza alcuna precauzione la propria chiave pubblica. Anche laddove un terzo intercetti la chiave, non potrà usarla per leggere i messaggi che Y invierà ad X ma, al massimo, per inviare anch'egli messaggi criptati ad X (cosa generalmente di ben scarso interesse). Questa inedita commistione tra pubblicità e segretezza, la sola idea di poter comunicare liberamente dati finalizzati ad operazioni crittografiche a sicurezza militare, risultò insopportabile ai dirigenti del GCHQ (General Communication Headquarters) l'organizzazione di intelligence britannica ove venne per la prima volta concepito il sistema a chiavi asimmetriche, alla fine degli anni Sessanta. Si temeva fondamentalmente che il sistema presentasse qualche falla sfuggita all'analisi. Anche alla luce della pesantezza computazionale di tali algoritmi in relazione alla potenza della macchine dell'epoca, il progetto venne abbandonato (cfr. S. LEVY, *Crypto*, Viking, New York 2001, p. 324).

L'utilizzo più ovvio è quello propriamente crittografico. Se Tizio desidera inviare a Caio un messaggio inviolabile per chiunque altro, gli è sufficiente criptare il messaggio utilizzando la chiave pubblica di Caio: solo quest'ultimo, che dispone della corrispondente chiave segreta, può leggere il messaggio. Non occorre previo accordo tra Tizio e Caio, e neppure che i due si conoscano: la chiave pubblica di Caio è a disposizione di tutti. Ancora più importante: non c'è bisogno di alcun canale di comunicazione sicuro tra Tizio e Caio, perché essi non debbono condividere alcuna informazione riservata; la chiave segreta di Caio deve essere utilizzata dal solo Caio, e non deve essere comunicata a chicchessia.

La sottoscrizione si realizza invece nel modo seguente. Il testo [54] da firmare resta in chiaro, leggibile per chiunque. Il medesimo testo viene pure criptato avvalendosi della chiave segreta del sottoscrivente; il messaggio in cifra che ne deriva è appunto la firma digitale, e viene acclusa al testo in chiaro [55]. La firma digitale di ciascun soggetto varierà pertanto a seconda del contenuto del messaggio: ciò ne impedisce l'uso fraudolento in calce ad un altro documento [56]. Il destinatario, o qualunque soggetto comunque interessato, procuratasi la chiave pubblica del mittente, confronta messaggio e firma digitale. Se il confronto dà esito positivo, due cose sono accertate. In primo luogo, il messaggio proviene sicuramente da quel mittente: solo lui (o lei) possiede la chiave segreta che consente di produrre una firma riconoscibile dalla chiave pubblica corrispondente. In secondo luogo, il messaggio non è stato alterato: se così fosse, non vi sarebbe più corrispondenza tra messaggio e firma [57]. Questo spiega perché un messaggio provvisto di firma digitale possa essere trasmesso anche attraverso reti intrinsecamente insicure (come Internet), senza che ci si debba preoccupare della possibilità di intercettazioni od alterazioni: come si è visto la firma, anche se intercettata, non è riutilizzabile, e le manipolazioni emergerebbero in sede di controllo.

---

[54] Che si tratti di un testo è solo l'ipotesi più semplice e comune. In realtà qualunque file di computer può essere criptato e/o provvisto di firma digitale: immagini, video, programmi, suoni.

[55] Si è operata una piccola semplificazione di comodo: in realtà, anche per evitare che ogni firma digitale sia lunga quanto il messaggio, si utilizza per le operazioni di firma digitale una sintesi automatizzata del messaggio stesso, detta hash. A voler essere particolarmente pignoli, vi è quindi necessariamente un numero indefinito di testi diversi tra loro cui si attaglia la medesima firma. La probabilità che uno di questi testi alternativi, ammesso che lo si possa ricavare, abbia un qualsivoglia significato in linguaggio naturale è però infinitesima: più facilmente si tratterà di qualcosa del tipo "lvJK1ib3gud m9s Lml0PokA". Che poi il testo alternativo, oltre a significare qualcosa, possa tornare in concreto utile all'eventuale manipolatore, è ipotesi del tutto inverosimile.

[56] Questa caratteristica è evidentemente indispensabile. Ciò fa sì, tra l'altro, che a questi fini siano inutilizzabili i sistemi biometrici, basati cioè sul riconoscimento dell'impronta digitale, della struttura della retina, della forma della mano, della voce e persino dell'odore. Simili tecnologie servono ottimamente allo scopo di impedire l'accesso a locali od attrezzature da parte di persone non autorizzate, ed in questo senso può contribuire alla sicurezza dei sistemi di firma digitale (cfr nota 19); ma se l'immagine biometrica venisse usata *tout court* come firma, sia il destinatario del documento così sottoscritto che qualunque malintenzionato in grado di intercettarlo, potrebbero riprodurla in maniera perfetta, giacché a quel punto si tratterebbe solo di una sequenza di bit come un'altra, copiabile alla stregua di un qualunque file. A maggior ragione, sono inservibili i sistemi basati esclusivamente sul PIN (Personal Identification Number), come il Bancomat.

[57] La comune firma digitale non protegge invece da un'altra eventualità: che qualcuno intercetti il file firmato, elimini la firma digitale originaria e la sostituisca con la propria. Potrebbe accadere per una domanda di brevetto, ad esempio. Propongono una soluzione A. MCCULLAGH ed altri, *Signature Stripping: A Digital Dilemma*, in *The Journal of Information, Law and Technology (JILT)* 2001/1.

Nulla vieta, naturalmente, di eseguire entrambe le operazioni sul medesimo messaggio, che sarà quindi firmato digitalmente e leggibile solo dal destinatario [58].

Per costruire un sistema compiutamente funzionante, occorre però risolvere un ulteriore problema: come può l'utilizzatore del messaggio essere certo del fatto che la chiave pubblica che sta impiegando per la verifica appartenga davvero a chi si presenta come sottoscrivente? Questo è uno snodo essenziale del sistema: è chiaro infatti che a nulla serve una tecnologia (praticamente) inviolabile sotto il profilo tecnico/matematico, se per la verifica si utilizzano dati non assolutamente attendibili. Per conseguire questo obiettivo, è necessaria, tuttavia, una struttura più articolata (detta PKI, Public Key Infrastructure), che comprenda un soggetto, dotato di terzietà ed imparzialità rispetto agli utenti, che certifichi l'autenticità delle chiavi e la corrispondenza della chiave pubblica con il suo titolare. E' la cosiddetta Certification Authority, o Autorità di Certificazione [59].

Nel modello più diffuso l'utente del sistema si reca presso un ufficio della Certification Authority, il quale provvede ad identificarlo e gli consegna un dispositivo di firma (per lo più una *smart card*) che contiene al suo interno la chiave segreta [60], inserendo poi la corrispondente chiave pubblica nell'apposito elenco e ad emettere il relativo certificato, accessibile via Internet a chiunque. La funzione di certificazione è separabile da quella diretta alla semplice acquisizione dei dati da pubblicare: in tal caso si parlerà di Registration Authority.

Il destinatario, onde eseguire la verifica del documento, impiegherà dunque la chiave pubblicata dall'Autorità di Certificazione sotto il nome del mittente; è garante della corrispondenza di quella determinata chiave privata (che di per sé non è altro che una sequenza di bit priva di senso proprio) ad una certa identità fisica [61]. L'operazione

---

[58] Non si tratta di una semplice esercitazione tecnologica: se intendo ad esempio impartire ordini alla mia Banca a proposito dei miei investimenti mobiliari, saranno egualmente desiderabili sia la certezza intorno alla provenienza dell'ordine che la riservatezza delle informazioni patrimoniali desumibili dal testo.

[59] Ciò fa sì che non si possano considerare firme digitali (almeno secondo la nozione prevalente quelle emesse nell'ambito del celeberrimo sistema PGP. Questo utilizza, è vero, la tecnologia a chiavi asimmetriche, ma non possiede la struttura gerarchica descritta nel testo, al cui vertice è posizionata la Certification Authority. Le chiavi pubbliche PGP circolano invece "orizzontalmente" da un utente all'altro del sistema. Alice e Bob si conoscono e nutrono reciproca fiducia; si scambiano (in ipotesi: di persona) le loro chiavi pubbliche. Se Alice invia a Bob (con un messaggio firmato elettronicamente) la chiave pubblica di Charlie, Bob, che come detto si fida di Alice, sarà verosimilmente disponibile a riconoscere come provenienti da Charlie tutti i documenti verificabili con quella chiave pubblica. E così via. Il sistema è detto *web of trust* (W. FORD e M. S. BAUM, *Secure Electronic Commerce*, Prentice Hall, Upper Saddle River, New Jersey, USA, 2000, p. 275): la certificazione non è centralizzata, ma dipende da relazioni che si sviluppano seguendo percorsi casuali all'interno della comunità degli utenti.

[60] Di regola le chiavi segrete, per ragioni di sicurezza, sono create direttamente all'interno dei dispositivi di firma (detti anche *tokens*) ed è impossibile estrarle dal dispositivo stesso. Normalmente il dispositivo consiste in una smart card, delle dimensioni di una carta di credito, ma esistono altri formati, come ad esempio degli spinotti tipo USB che ospitano al loro interno tutto l'occorrente, e che hanno il vantaggio di essere collegabili direttamente alla grande maggioranza dei computers, senza la mediazione di un lettore. Che il procedimento di generazione delle chiavi sia fisicamente attivato dall'utente o dalla Certification Authority non è circostanza determinante ai fini della sicurezza dell'insieme, almeno sino a quando la chiave segreta generata resta inaccessibile all'Authority stessa, che non ha alcun motivo per entrarne a conoscenza.

[61] Anche se talora è ammesso che la persona fisica sia indicata con un pseudonimo: così in tutte le legislazioni dell'Unione Europea, a seguito della direttiva dell'Unione Europea 1999/93/CE Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro

di verifica, come già accennato, consente pure di accertare che il documento non è stato in alcun modo manipolato. I dati necessari sono contenuti in un certificato, che è a sua volta firmato digitalmente.

La Certification Authority svolge altresì un'ulteriore importante funzione: quella di gestione della revoca o sospensione del certificato di firma. Si procede a revoca ogniqualvolta il titolare abbia perso il controllo del dispositivo di firma, ad esempio per smarrimento, distruzione, sottrazione, furto o guasto, oppure si nutra sospetto di abusi o falsificazioni [62]. Alla sospensione si ricorre qualora occorra un blocco temporaneo, oppure come rimedio d'urgenza mentre sono in corso gli accertamenti per la revoca definitiva. Secondo il modello più accreditato, è onere di chi ha interesse a valersi del documento firmato eseguire una verifica in base alle risultanze aggiornate della Certification Authority. Una firma emessa in base ad un certificato sospeso o revocato è quindi inopponibile al titolare, e per lo più è considerata come una "non firma", *tout court*.

Le Certification Authorities, per prassi internazionale, redigono un Certification Practice Statement, detto in italiano Manuale Operativo, ove sono contenute le regole cui la Certification Authority si attiene nella sua attività [63].

2. L'equiparazione tra firma digitale ed autografa

Come accennato, il legislatore italiano del 1997 operò la piena equiparazione dei documenti provvisti di firma digitale a quelli cartacei con firma autografa. Questa scelta è stata adottata da svariate altre legislazioni nel mondo. A dispetto della sua apparente razionalità e semplicità, tale impostazione reca con sé un considerevole bagaglio di difficoltà. La firma digitale, come si tenterà di evidenziare nei punti che seguono, è qualcosa di intrinsecamente diverso dalla firma autografa: tentare di azzerare queste differenze *per rescriptum principis* genera, nella migliore delle ipotesi, incertezze ed incongruenze.

2.1. Atti sottoscrivibili

Dal punto di vista tecnico ogni *file* di computer (poco importa che contenga testo, immagini, spezzoni video o musica) è suscettibile di firma digitale. Anche il prodotto dell'operazione di firma è solo un *file* come un altro, come tale suscettibile di copia. Ma per il giurista i problemi iniziano appunto qui. L'espressione tecnico/informatica "copia di un *file*" indica un'operazione che dal punto di vista concettuale è ben diversa dalla

---

comunitario per le firme elettroniche (*Gazzetta Ufficiale delle Comunità europee* n. L 013 del 19 gennaio 2000 pagg. 12/20).

[62] Secondo alcune stime, la gestione degli elenchi dei certificati revocati (cosiddette CRL, *Certificate Revocation List*) rischia però di trasformarsi in un serio problema, a causa della quantità di dati e di potenza di elaborazione richiesta. Una soluzione è stata proposta da S. MICALI, docente al Massachusetts Institute of Technology: si veda *NOVOMODO: Scalable Certificate Validation and Simplified PKI Management*, relazione presentata nell'aprile 2002 al *1st Annual PKI Research Workshop* presso l'Università di Dartmouth.

[63] Difficile da qualificare la loro esatta natura giuridica, ma pare di potersi prima facie prudenzialmente affermare che il loro contenuto non sia opponibile, in linea di principio, ai terzi, con ciò confinandoli al ruolo di fonte del rapporto contrattuale che lega certificatore e soggetto certificato. Certamente i terzi potranno però, secondo i principi, valersi delle risultanze dei manuali quando a loro favorevoli: nessun dubbio, ad esempio, che la previsione contenuta nel Manuale Operativo del notariato italiano, secondo cui tutti i soggetti certificati dal Consiglio Nazionale del Notariato sono notai in esercizio, possa essere fatta valere da chiunque vi abbia interesse.

copia di un documento cartaceo. Quest'ultima consiste nella realizzazione di un prodotto, la copia, cui resta intrinseca la derivazione genetica dall'originale, che a sua volta resta tendenzialmente riconoscibile come tale; la cosiddetta operazione di copia di un *file*, se non incontra errori, equivale invece a realizzare duplicati identici del *file* originale, in numero illimitato. La cosa, a ben vedere, non dovrebbe sorprendere: un *file* non è altro che un insieme di bit, o se vogliamo una sequenza di caratteri. Pretendere di distinguere originale e copia di un *file* equivale ad affermare che scrivendo le parole *Dante Alighieri* io non ottenga il *vero* nome di un poeta, ma solo una *copia* del suo nome. Ne discende l'impossibilità di utilizzare la firma digitale per cambiali od assegni: anche il documento firmato digitalmente (che, come si è detto, è solo un *file* come un altro) è duplicabile all'infinito senza alcuna variazione. Non è ovviamente pensabile una cambiale digitale riproducibile in infiniti esemplari, tutti a pari titolo *originali* [64]. In termini generali, può affermarsi che non è suscettibile di firma digitale ogni atto la cui incorporazione in un documento ha una specifica valenza giuridica. La normativa italiana tace però su questo punto, come fanno peraltro diverse altre legislazioni.

Questo esempio, oltre ad illuminare un profilo di non coincidenza tra firma digitale e firma autografa, suggerisce *en passant* una modesta considerazione di metodo. Un'affermazione tecnicamente ineccepibile può divenire gravemente inesatta se trasportata in un contesto giuridico: *ogni file è suscettibile di essere firmato digitalmente* è affermazione tecnicamente esatta, *ogni documento è suscettibile di essere firmato digitalmente* è affermazione giuridicamente errata. Non è lecito dunque al giurista abdicare ad una parte fondamentale della sua funzione, che è quella di studiare, comprendere e *giuridicamente* qualificare le realtà con le quali ha la ventura di misurarsi. Non è possibile arrestarsi sulla soglia, affidando ai tecnici la cognizione del fenomeno informatico: l'esito, paradossale se si vuole ma in qualche modo inevitabile, è l'enunciazione da parte del giurista di concetti tecnicamente corretti ma giuridicamente imprecisi od incompleti, quando non francamente indifendibili.

2.2. La provenienza del documento firmato

In letteratura si rinvengono frequentemente valutazioni iperboliche intorno all'affidabilità della firma digitale. Si può accettare senz'altro un assunto: la tecnologia descritta consente di dar certezza, con un livello di attendibilità senza precedenti, che un determinato documento è stato firmato avvalendosi di una determinata chiave di firma. Eseguita con esito favorevole la verifica (in senso informatico) di una firma digitale, potremo dire quindi, ad esempio, di poter essere certi al di là di ogni ragionevole dubbio che un certo documento è stato firmato avvalendosi di una ben individuabile chiave di firma.

Tale chiave di firma, anche se inizialmente nel pieno controllo del suo titolare, può successivamente sfuggire al suo controllo, per volontà del titolare o meno. A differenza di quanto accade con una firma autografa tradizionale, la firma digitale non serba alcuna traccia della fisica identità di chi ha manovrato il dispositivo, onde è praticamente del tutto impossibile fornire la prova, ex post, di chi abbia concretamente

[64] A tale difficoltà si tenta di rimediare ricorrendo ad infrastrutture complesse: nella soluzione più nota ciò ha luogo attraverso l'intervento di un sistema esterno che funga da terzo garante, il TCU (Trusted Custodial Utility). A differenza delle legislazioni europee il Titolo II dell'Electronic Signatures in Global and National Commerce Act (normativa federale USA) riconosce tale figura, limitandola però ai titoli forniti di garanzia ipotecaria. Si veda in generale sull'argomento J.K. WINN, *What Is a 'Transferable Record' and Who Cares?* in *BNA Electronic Commerce & Law Report 1060* (October 25, 2000).

apposto una determinata firma [65]. Molto appropriatamente, nella dottrina italiana era stata affacciata la proposta [66] di adottare la definizione di sigillo informatico, che meglio corrisponde alla natura intrinseca del fenomeno: l'idea non ha però avuto successo.

Questa semplice constatazione comporta una conseguenza giuridica estremamente importante. Le legislazioni che attribuiscono valore giuridico alla firma digitale lo fanno sulla base di un *sistema convenzionale di imputazione di effetti giuridici*. Non è corretto insomma affermare che la firma digitale attesti la provenienza di un documento da una determinata persona [67]: nel mondo cartaceo è sempre possibile eseguire una perizia calligrafica, che qui non ha al momento [68] corrispondente alcuno. Sotto questo profilo la legislazione italiana (e di molti altri Paesi) in materia di firma digitale pone in essere una peculiare operazione concettuale [69], a ben vedere, imputando il documento su una base puramente convenzionale e non a fronte della realtà storica dell'effettiva apposizione della sottoscrizione.

---

[65] In linea di principio alla difficoltà potrebbero porre rimedio le tecniche di riconoscimento biometrico, basate sull'identificazione di caratteristiche fisiche (iride, impronta digitale, voce, struttura del viso, persino l'odore). Il problema non è tanto l'attuale livello di affidabilità della tecnologia, che pure ha riservato qualche cattiva sorpresa: il professor T. MATSUMOTO, dell'Università di Yokohama, ha dimostrato ad esempio che sistemi di riconoscimento delle impronte digitali, fino ad allora considerati molto sicuri, possono essere violati utilizzando tecnologie assolutamente casalinghe (l'episodio è stato riportato, tra gli altri, dalla BBC di Londra il 17 maggio 2002). Trattandosi, nel caso della firma digitale, di un accorgimento di sicurezza aggiuntivo, l'inconveniente è sopportabile, ma almeno due difficoltà ben più serie al momento si frappongono. Occorrerebbe in primo luogo lo sviluppo di protocolli standard che consentano di integrare i dati biometrici nella smart card. I dispositivi comunemente disponibili in commercio hanno tutt'altra funzione, giacché bloccano l'accesso a determinati computers od apparati, e non precluderebbero dunque l'impiego della smart card su altri apparecchi. In secondo luogo, quello che in altri contesti è un punto di forza delle tecniche biometriche, e cioè il fatto che l'impronta digitale ed altri dati biometrici non cambino mai (o cambino molto lentamente) può trasformarsi in un boomerang: se qualcuno trova il modo di recuperare dalla memoria di un computer l'impronta digitale di Tizio, potrà con ottime possibilità di successo usarla, un'ora o dieci anni dopo, per ingannare un altro sistema. Con l'aggravante che una smart card rubata si può bloccare e sostituire: un'impronta digitale? A questo si tenta di rimediare con tecnologie complesse, in cui il dato biometrico viene mediato attraverso un sistema crittografico, cosicché i dati scambiati tra gli apparati coinvolti nel procedimento di identificazione varino ad ogni sessione.

[66] S. MICCOLI, *La sicurezza giuridica nel commercio elettronico* (tesi di laurea), reperibile in Rete (formato Word) alla pagina http://web.tiscalinet.it/conoge/silmic.doc, seguita da D. GIAQUINTO e P. RAGOZZO, *Il sigillo informatico*, in *Notariato*, 1997, 80; vedasi però soprattutto M. MICCOLI, *Commercio telematico: una nuova realtà nel campo del diritto*, IPSOA, Milano 1998, p. 35. C. REED, *What is a Signature?*, in *The Journal of Information, Law and Technology (JILT)*, 2000 (3), http://elj.warwick.ac.uk/jilt/00-3/reed.html/ paragona la firma digitale ad un semplice timbro di gomma (*rubberstamp*), mentre S. MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 318, avvicina la firma digitale ad un particolare tipo di sigillo in uso in Giappone sin dall'ottavo secolo, lo *Jitsuin*.

[67] No form of electronic signature is capable of linking the use of a signature to a particular person. Unless the sending party confirms they sent the message or document with the signature attached, the recipient cannot determine whether the sending party authorized the use of the signature (nessuna firma elettronica può collegare l'uso della firma ad una determinata persona. A meno che il mittente non confermi d'aver inviato il messaggio firmato, il destinatario non può stabilire se il mittente ha autorizzato l'uso della firma) S. MASON, Electronic Signatures in Law, LexisNexis UK, London 2003, p. 348.

[68] Almeno, come detto, sino all'introduzione di tecnologie biometriche.

[69] Così anche S. MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 7. Operazione peraltro non priva di precedenti nel sistema italiano: si pensi al caso del telegramma non sottoscritto ma *fatto consegnare* all'Ufficio telegrafico (articolo 2705 del codice civile).

Va quindi considerata la possibilità che la firma venga apposta senza che tale evento corrisponda ad un'espressione di volontà del titolare del certificato. Ciò può dipendere da una pluralità di ragioni, che si potrebbero forse, molto approssimativamente, distinguere in due gruppi: rischi di origine umana e rischi di origine tecnica. Ma a guardare bene, dato tecnico e dato umano sono indissolubilmente intrecciati, e si commetterebbe un grave errore nel voler separare l'uno dall'altro.

2.2.1. I rischi di origine umana: le Autorità di Certificazione

L'osservazione è banalissima, ma cionondimeno (o forse proprio per questo) stranamente trascurata [70]: la catena che unisce il titolare Tizio al documento firmato, che consente di imputare il documento a Tizio, si compone di due anelli: il test informatico che permette di stabilire che una determinata firma è riferibile ad un determinato certificato, e l'identificazione fisica del richiedente compiuta al momento del rilascio del certificato stesso, in base alla quale si può affermare che fu Tizio, e non altri, a richiederne l'emissione. Anche tralasciando per il momento i rischi insiti nel primo passaggio, resta il fatto indubitabile che la fisica identificazione del richiedente non è diversa da quella compiuta in ogni altro contesto [71]. Ed ogni catena, per definizione, non può essere più solida del più debole dei suoi anelli [72]. Le legislazioni che attribuiscono un determinato valore ai documenti provvisti di firma digitale, solo apparentemente si limitano quindi a disciplinare il fenomeno *tecnologico* noto come firma digitale, ma attribuiscono (per implicito, ma in modo non per questo meno incisivo) una specifica valenza giuridica all'operato di determinate persone fisiche.

---

[70] Soprattutto dalla dottrina italiana, anche se con le dovute eccezioni degli studiosi più attenti, come R. ZAGAMI, *Firma digitale e sicurezza giuridica*, cit, p. 271. Gli specialisti statunitensi, in generale, sembrano sotto questo profilo meno entusiasti e più realisti. Si prenda ad esempio C. M. ELLISON e B. SCHNEIER *(Ten Risks of PKI, cit.*): *Security is a chain; it's only as strong as the weakest link. The security of any CA-based system is based on many links and they're not all cryptographic. People are involved. Does the system aid those people, confuse them or just ignore them? Does it rely inappropriately on the honesty or thoroughness of people?* (La sicurezza è una catena, solida solo quanto il più debole dei suoi anelli. La sicurezza di ogni sistema di CA è basata su molti passaggi, e non tutti sono crittografici. Sono coinvolte persone. Il sistema aiuta queste persone, le confonde o magari le ignora? Fa inappropriatamente affidamento sulla onestà o coscienziosità della gente?).

[71] Affidata cioè all'identificazione di una persona fisica eseguita da un'altra persona fisica. L. V. MOSCARINI, in *Commentario* (con C. M. BIANCA ed altri) *al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 680/681, in più passaggi afferma che l'identificazione del soggetto è operata dal server, spingendosi sino ad affacciare l'ipotesi di "abuso perpetrato dal server" (*sic*), che a quanto ci consta appartiene non al diritto ma alla fantascienza.

[72] Non pare tenerne conto, tra gli altri, L.M. DE GRAZIA, Comunque dovremo andare dal notaio di persona!, in Interlex 27/10/97, http://www.interlex.it/conv97/degrazi3.htm: Per dirla in altre parole, oggi è sicuramente più difficile alterare una firma digitale crittografata che spacciarsi per qualcun altro davanti ad un notaio esibendo documenti e testimoni falsi, con buona pace della perfetta buona fede dei Notai. Che la tecnologia crittografica della firma digitale a chiavi asimmetriche sia in assoluto più sicura del riconoscimento fisico operato sulla base di un documento è affermazione condivisibile, ma l'Autore trascura che, come evidenziato nel testo, anche l'iter della firma digitale contempla un riconoscimento fisico, compiuto da soggetto senz'altro meno qualificato del notaro. A meno che non si affermi che il dipendente della Registration Authority (su cui infra nel testo) sia, chissà perché, soggetto più affidabile del notaro, ne discende pianamente che la firma digitale è intrinsecamente meno sicura di una firma autenticata.

L' accertamento dell'identità personale del titolare del certificato compete alla Certification Authority [73], che in Italia, come nella maggior parte dei Paesi, è un operatore privato.

Sin da questa semplice considerazione discende l'improponibilità dell'equiparazione, pure talora tentata, tra firme digitali e firme autenticate da notaio. Occorrerebbe, in primo luogo, che il personale della Certification Authority abbia le medesime caratteristiche di attendibilità del notaio, e che le relative prassi siano di equivalente affidabilità [74]. Ma neppure questo sarebbe del tutto soddisfacente. Chi desideri vedere autenticata la propria firma da un notaio, deve dinanzi a lui comparire in occasione della sottoscrizione di ciascun documento. Il rilascio del dispositivo di firma digitale avrebbe una valenza addirittura superiore, giacché attribuirebbe uno status giuridico privilegiato a tutta l'indefinita serie di documenti che in base a quel certificato saranno firmati [75].

Superfluo poi annotare che, nel sistema di notariato latino, l'identificazione del sottoscrivente è solo una fase, e forse la meno caratterizzante in assoluto, dell'intervento notarile, che ha il suo fulcro altrove: nel controllo di legalità, nell'indagine della volontà delle parti, nell'assistenza loro fornita, nella redazione di un documento che realizzi la loro volontà in modo giuridicamente corretto. Sotto tutti tali profili, la firma digitale non è di alcun aiuto.

Frutto di confusione e di scarsa conoscenza dello strumento è anche l'affermazione, che pure talvolta si incontra, secondo cui la firma digitale dispenserebbe dalla personale comparizione dinanzi al notaio. Ciò potrà forse essere possibile in futuro con l'ausilio di sistemi particolarmente avanzati di teleconferenza, che consentano un

---

[73] La normativa italiana stabilisce che il certificatore è obbligato a *identificare con certezza la persona che fa richiesta della certificazione* (articolo 29 bis del citato TU 445/2000).

[74] Inutile dire che i riscontri offerti dalla prassi sono di tutt'altro tono. L'incidente più celebre ha visto come illustre protagonista VeriSign, società californiana leader mondiale del settore, che ha inavvertitamente rilasciato ad impostori due certificati intestati nientedimeno che a Microsoft, il 29 e 30 gennaio 2001 http://www.microsoft.com/technet/security/bulletin/MS01-017.asp Si trattava di due prestigiosi certificati *VeriSign Class Three*, destinati all'autenticazione dei programmi per computer. In concreto, avrebbero potuto essere utilizzati per inviare a qualunque utente di software Microsoft, ovunque nel mondo, sedicenti aggiornamenti di programmi esistenti, che il browser Microsoft Internet Explorer avrebbe espressamente garantito come provenienti da Microsoft stessa. Anche l'utente accorto avrebbe quindi proceduto senz'altro allo scaricamento, installando così nel proprio sistema qualunque tipo di programma (con funzione di spionaggio, ad esempio) al mittente fosse piaciuto. Ma non è tanto l'incidente (che può accadere sempre ed ovunque) ad attirare l'attenzione, quanto il contesto in cui è maturato. In quell'occasione si è appreso infatti che le due società statunitensi si affidavano per tale delicata funzione di certificazione a semplici conferme telefoniche, e che Microsoft Internet Explorer procedeva in automatico alla conferma della genuinità della firma senza previamente verificare se il certificato VeriSign non fosse stato eventualmente revocato.

[75] Anche lo statunitense Brad BIDDLE, Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure, in San Diego Law Review (33) 1143, 1996, sottolinea: digitally-signed documents do not achieve the same assurances of genuineness that documents signed in the personal presence of a notary achieve, and should not be given the same legal status (i documenti firmati digitalmente non forniscono le medesime garanzie di autenticità di quelli sottoscritti alla personale presenza del notary public, e non dovrebbe esser loro attribuito il medesimo status giuridico). Da notare che qui si allude all'autentica del notary public americano, figura sprovvista (tra l'altro) di qualsivoglia qualificazione giuridica: è per lo più sufficiente avere 18 anni, essere incensurati e conoscere l'inglese. Persino un intervento qualitativamente così modesto è reputato dall'Autore (difficilmente sospettabile di un approccio neoluddista, facendo egli parte dello staff legale di Intel) più affidabile della firma digitale.

dialogo tra notaio e comparente di cristallina trasparenza, tale da permettere al notaro di svolgere con sicurezza la sua funzione di indagine e consulenza. Ma ciò poco o nulla ha a che vedere con la firma digitale.

2.3. Solennità della sottoscrizione

Perplessità possono essere formulate anche su un piano più generale. E' legittimo chiedersi se le operazioni informatiche richieste per l'apposizione della firma digitale (qualche rapido click di un mouse e la digitazione di un PIN) siano idonei a soddisfare l'altra tradizionale funzione attribuita alla forma, la responsabilizzazione del soggetto cui il documento sarà riferibile. La firma digitale propriamente detta ha un'articolazione che conferisce al gesto della sottoscrizione un più che rispettabile grado di solennità, ma che forse può essere concretamente apprezzato solo da chi abbia ricevuto un'adeguata formazione sulle caratteristiche ed il funzionamento del sistema.

E' ben vero che in tutto il mondo sono di uso corrente presso il grande pubblico sistemi che, sulla base di una semplice identificazione informatica, eseguono operazioni anche di non trascurabile valore economico: è il caso dei sistemi ATM, di *home banking* o di commercio elettronico. Ma si tratta di sistemi limitati, nel senso che la loro operatività è circoscritta a rapporti giuridici predeterminati, e spesso ad un ammontare massimo predefinito. Tali sistemi hanno inoltre modalità operative tali da attirare comunque l'attenzione dell'utente sul tipo di atto che si pone in essere. Accostarsi ad uno sportello ATM, collegarsi con il sito web della propria banca, sono gesti che per loro stessa natura convogliano l'attenzione dell'utente sulle operazioni che potranno aver luogo. I softwares impiegati hanno per di più una struttura dialogica, e sottopongono (ripetutamente, per lo più) i termini dell'operazione all'utente attraverso ben percepibili videate.

Nulla di tutto ciò nella firma digitale: per lo più le procedure impiegate richiedono semplicemente che si digiti il nome del *file* da sottoporsi a firma. Un'operazione spesso completamente al buio, che si affida solo alla corretta identificazione dell'indirizzo informatico che il file desiderato ha sul computer impiegato: non vi è insomma garanzia alcuna che il contenuto del documento firmato fosse accessibile o visibile all'utente al momento dell'apposizione della firma.

2.4. Accessibilità

Il concetto di accessibilità o visibilità del documento merita un accenno, essendo meno ovvio di quanto appaia a prima vista. Un determinato file può essere visualizzato in maniera diversa da programmi diversi. I files html, quelli che compongono l'ossatura del World Wide Web, sono ad esempio riprodotti in modo assai diverso dai vari browsers (Netscape Navigator, Opera, Microsoft Internet Explorer e così via): avviene di frequente che intere sezioni del testo siano invisibili sul monitor, e ridiventino visibili laddove si decida di stampare la pagina. Non sempre ciò che appare a video, dunque, è ciò che si sta firmando.

Alcuni tipi di file, e soprattutto quelli noti come *.doc*, prodotti con il programma Microsoft Word [76], contengono poi una quantità enorme di dati, di cui l'utente (anche mediamente competente) non è a conoscenza, ma che possono essere di straordinaria

[76] Formato che, per le ragioni che appariranno chiare nel prosieguo, non è utilizzabile per testi destinati alla firma digitale, salvo speciali adattamenti. I notai italiani firmano digitalmente solo files pdf ed xml.

delicatezza [77]. E' ben vero che simili infortuni accadono indipendentemente dalla firma digitale, ma quel che qui interessa è che tutti questi dati, in quanto ricompresi nel file, sarebbero tecnicamente parti del documento firmato, a totale insaputa dell'utente [78].

Ma vi è di più. In tali files possono essere inseriti i cosiddetti campi dinamici, cioè campi che possono essere configurati per aggiornarsi automaticamente all'apertura del documento e il cui valore è impostato in apposite variabili all'interno di Word o del sistema operativo del computer in uso. Possibili campi sono la data, l'ora, il nome del documento, l'autore. Si può ad esempio istruire il programma affinché ad un certo punto di un testo inserisca la data del giorno. Prendiamo un utente che il primo settembre si trovi a firmare un documento così prodotto: leggendo il suo documento su Microsoft Word, vedrà la data del giorno, e firmerà il file. Ma attenzione: il file in sé non contiene tale data: contiene un'istruzione informatica, impartita al computer, di inserire, a quel punto del testo, la data del giorno. E' il *word processor*, nel nostro esempio Microsoft Word, a visualizzare la data, che nel file non c'è. Riprendendo quel file digitalmente firmato un mese dopo, allo stesso punto del testo si leggerà *primo ottobre*. E questo non in quanto il documento firmato sia stato alterato, ma in quanto l'utente, sempre senza saperlo, non ha firmato un testo, ma un'istruzione, un frammento di software [79].

2.5 Intrusione

Una semplice imprudenza nella gestione del proprio computer può dunque esporre chiunque, anche se sprovvisto di specifiche cognizioni tecniche, a dover rispondere degli effetti giuridici di una serie indefinita di documenti di cui non ha mai avuto cognizione [80]. Si finisce, tra l'altro, col porre indirettamente a carico del *quisque de*

---

[77] La cronaca non è avara di incidenti celebri: due tra i più recenti. Il 23 dicembre 2003 *CNN* ha riferito del rilascio, da parte della US Court of Appeals del Secondo Circuito, di una versione in formato Microsoft Word della sua decisione del giorno 18 nel caso di José Padilla, un sospetto terrorista trattenuto dalle forze armate USA senza alcun provvedimento giudiziale benché si trattasse di un cittadino statunitense arrestato a Chicago in relazione ad un presunto tentativo di attacco terroristico da compiersi in territorio americano. Tale file conservava traccia di una modifica apportata in corso d'opera al punto cruciale della questione, di grande rilevanza politica per la Casa Bianca: la definizione di Padilla quale *combattente nemico catturato,* strada facendo era stata dai giudici modificata in *sospettato detenuto*. Nel gennaio dello stesso anno, sul sito web di Downing Street veniva pubblicato un rapporto ufficiale sulla guerra in Iraq, sempre in formato Microsoft Word, che ad un'analisi accurata rivelava i nomi di alcuni collaboratori che avevano partecipato alla redazione del testo (così Michael WHITE e Brian WHITAKER, *UK war dossier a sham*, in *The Guardian*, 7 febbraio 2003). Secondo una fonte (Paolo ATTIVISSIMO, *Tony Blair scottato da Word*, in *Apogeoonline* 30 luglio 2003) dal file si può anche desumere l'informazione che tal Pratt ha fornito il dossier a tal Blackshaw affinché lo facesse pervenire a Colin Powell, e che lo ha fatto usando un floppy.

[78] Sembra lecito supporre che ciò che è sfuggito ai responsabili dei sistemi informatici del Capo del Governo di Sua Maestà Britannica (vedi nota precedente) possa talora sfuggire anche all'utente medio.

[79] A. GELPI, *La firma è sicura, il documento no*, In *Interlex*, http://www.interlex.it, 19 settembre 2002. Dopo la diffusione di questa ed altre consimili analisi, Microsoft Italia annunciò lo sviluppo di appositi software destinati a rendere anche i files Word idonei alla firma digitale (comunicato stampa del 30 gennaio 2003). Sull'argomento M. CAMMARATA ed E. MACCARONE, *La firma digitale sicura*, Giuffrè, Milano 2003, p. 250.

[80] E' lo scenario noto tra gli specialisti come *Grandma picks the bad password and loses her house* (La nonna sceglie la password sbagliata e perde la casa); l'espressione è riferita tra gli altri da B. BIDDLE, *A short history of "digital signature" and "electronic signature" legislation*, in S. GARFINKEL e G. SPAFFORD, *Web Security, Privacy And Commerce*, O'Reilly, Cambridge (Massachusetts, USA) 2001.

populo l'onere di gestire i propri strumenti informatici secondo standard di tipo professionale, il che pare decisamente troppo [81].

3. Il regime probatorio

Il regime probatorio della firma digitale propriamente detta, come disegnato dall'attuale legislazione italiana, appare ben lungi dall'offrire una sistemazione soddisfacente della problematica. Non è stata, beninteso, affermata l'equivalenza piena tra firma autenticata e firma digitale, con ciò escludendo, tra l'altro, che una firma digitale senza intervento del notaio possa essere utilizzata per atti destinati alla pubblicazione nei Registri Immobiliari o nel Registro delle Imprese. Ma anche la semplice equivalenza con la firma autografa è ben lungi dal risultare aproblematica.

Abbiamo osservato come sia di fatto impossibile fornire la prova di quale persona fisica abbia concretamente apposto una determinata firma digitale. Per altro verso, abbiamo notato come il rischio che la firma venga apposta in modo indipendente dalla volontà del titolare sia tutt'altro che teorica [82].

Se trasportiamo questo semplicissimo dato sul piano probatorio, la nebbia si fa fitta. E' particolarmente arduo pretendere che chi intende valersi della firma provi che il congegno è stato davvero manovrato dal titolare: salvo casi eccezionalissimi, come potrebbe? Equivarrebbe in pratica ad azzerare il valore giuridico della firma digitale. Ogni altra strada conduce a far gravare sul titolare, su base oggettiva, il rischio di ogni uso improprio del certificato di firma digitale da lui fatto emettere. Anche riconoscendo al titolare margini di prova contraria, questi risulterebbero infatti di interesse poco più che scolastico: non si vede come potrebbe verosimilmente dimostrare di non essere stato l'autore della firma. Neppure la prova di essersi trovato dalla parte opposta del globo sarebbe di qualche utilità, atteso che un documento provvisto di firma digitale può essere inviato ovunque in una frazione di secondo, grazie alla posta elettronica. Non si pensi alle ipotesi di smarrimento e sottrazione del dispositivo di firma, perché quelle sono coperte dalle apposite procedure di sospensione e revoca; l'uso di un certificato revocato o sospeso equivale ad una "non firma", e quindi il problema è azzerato alla radice.

Qualunque approccio legislativo che si limiti ad intervenire in modo rigido sullo status probatorio della firma digitale è destinato a non produrre un assetto soddisfacente, ma si limita a far gravare su questo o quel soggetto i costi delle disfunzioni del sistema [83].

---

[81] Rileva S. MASON, Electronic Signatures in Law, LexisNexis UK, London 2003, p. 91, che il sistema involves the acceptance of risk by the user. However, the nature and extent of the risk is not made clear, and it is high improbable that ordinary users will have the knowledge, skill and resources to manage such a risk (implica l'accettazione di rischi da parte degli utilizzatori. La natura e la gravità di tali rischi non sono chiare, ed è molto improbabile che gli utenti comuni posseggano conoscenze, abilità e risorse sufficienti a gestirli).

[82] La dottrina italiana prevalente considera tali firme comunque riferibili al titolare in applicazione di un generale principio dell'*apparenza imputabile*, dacché la situazione di apparente provenienza del documento dal titolare della chiave di firma deriverebbe comunque da comportamenti (o negligenze) a lui imputabili. A.M. GAMBINO, voce *Firma Digitale*, in *Enciclopedia Giuridica Treccani*, Roma 1999, p. 9; C. M. BIANCA *Commentario al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 670.

[83] Alcune legislazioni si pongono l'obiettivo di una maggior flessibilità, come l'Uniform Electronic Evidence Act canadese, del 1998, che alla sezione 3 stabilisce *The person seeking to introduce an electronic record has the burden of proving its authenticity by evidence capable of supporting a finding*

Il problema, a giudizio di chi scrive, è intrinseco: non vi è equivalenza di fatto tra un sistema, come la firma autografa, che documenta la fisica provenienza di un documento da un soggetto, ed un sistema, come la firma digitale, che realizza un'imputabilità del documento su base puramente convenzionale. Ogni tentativo di equiparazione conduce con sé un inevitabile carico di forzature e difficoltà [84].

E' probabile che, lasciato a se stesso, l'assetto normativo che si è andati descrivendo possa comunque incontrare elementi di riequilibrio. In particolare, è legittimo attendersi un atteggiamento particolarmente morbido da parte della giurisprudenza qualora si tenti di far gravare su soggetti non professionali i rischi di malfunzionamento del sistema. Questo è tanto più probabile nelle ipotesi in cui l'uso della firma digitale sia reso obbligatorio, ad esempio nei rapporti con i pubblici uffici. E' infatti razionale, anche sul piano economico, che i rischi intrinseci ad un determinato sistema di documentazione e comunicazione gravino su chi sceglie, per sua comodità o vantaggio, il sistema stesso: questa è la ratio sottesa alle soluzioni legislative adottate in molti ordinamenti. Far ricadere i rischi di malfunzionamento sul mittente laddove il sistema sia stato prescelto dal destinatario rompe tale logica [85].

E' altrettanto verosimile [86] che un giudice possa esitare dinanzi a documenti di importanza tale da far ritenere non appropriato il ricorso alla sola firma digitale. Indica tale direzione la già ricordata Direttiva dell'Unione Europea 1999/93/CE, che all'articolo 6 riconosce tutela al terzo a condizione che abbia fatto *ragionevole* affidamento sul certificato; l'espressione è trasfusa intatta nell'articolo 28bis del DPR445/2000 [87].

La norma è dettata in materia di responsabilità del certificatore, ma pare imporre al terzo un onere di diligenza e ponderazione che non può non avere una sua valenza più generale.

Appartiene alle scelte discrezionali di ciascun legislatore reputare o meno questo sistema di imputazione convenzionale un idoneo equivalente della sottoscrizione autografa tradizionale, ed il legislatore italiano, come accennato, ha dato una risposta affermativa. Una scelta che *prima facie* si fa apprezzare per la propria linearità, e per la simmetria che si viene a creare tra firma autografa e digitale; ad una più approfondita analisi non va però esente da perplessità.

Non v'è dubbio che in molti casi tale approccio appaia opportuno. E' per altro verso perfettamente razionale che un imprenditore commerciale, che utilizzi il sistema per le transazioni d'affari della sua impresa, sia in tale ambito senz'altro vincolato dall'attività negoziale posta in essere con la sua firma digitale, anche laddove ciò sia avvenuto a sua insaputa o contro le disposizioni da lui impartite. Può naturalmente accadere che si abbia una falla nella sicurezza del sistema informatico, oppure che la

---

that the electronic record is what the person claims to be (Chi intende far valere un documento elettronico ha l'onere di provare la sua autenticità con ogni mezzo di prova idoneo a dimostrare che il documento elettronico è realmente ciò che si assume che sia).

[84] Tali elementi sono presenti nel corrente dibattito italiano, nel quale è stata ripetutamente affacciata, anche da autorevoli fonti governative, l'opportunità di una sorta di passo indietro.

[85] S. MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 311.

[86] In tal senso pure S. MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 351.

[87] Si muove in tale ambito il Manuale Operativo relativo ai servizi di certificazione del Consiglio Nazionale del Notariato italiano, quando precisa che *l'esistenza e la validità del certificato non dispensano però l'utente dall'eseguire ogni altra verifica che appaia opportuna secondo criteri di oculata prudenza, anche in relazione al rilievo, economico o d'altra natura, degli interessi coinvolti.*

smart card venga sottratta insieme al PIN dalla cassaforte ove è custodita, oppure ancora che il dipendente addetto all'utilizzo del sistema di firma lo utilizzi in modo infedele, o infine che non sia stata correttamente attivata la procedura di revoca del certificato in caso di smarrimento. Ma in tutti questi casi è del tutto ragionevole, e conforme a diffusi principi di diritto commerciale, che l'imprenditore risponda dell'attività giuridica così posta in essere.

Ma in un contesto di equivalenza piena ed illimitata tra firma digitale e firma autografa possono prospettarsi ipotesi assai meno tranquillizzanti. Riprendendo l'esempio appena fatto, il dipendente infedele potrà, ad esempio, alienare validamente l'abitazione privata dell'imprenditore.

Può in quest'ottica però prevedersi che i certificati di firma digitali possano essere emessi con limiti di importo o con validità limitata solo a determinate categorie di operazioni, ipotesi peraltro già prevista [88] dalla normativa italiana. Così un imprenditore che intenda utilizzare la firma digitale per concludere via Internet contratti per l'approvvigionamento di merci, ed ottenga un certificato di firma *ad hoc*, non sarebbe giuridicamente vincolato da un contratto di vendita immobiliare.

4. La delega de facto

Con l'affidamento consapevole della chiave di firma ad un terzo il titolare può realizzare in modo assai semplice una delega *de facto* della propria firma; come già accennato, le firme così apposte saranno assolutamente indistinguibili da quelle apposte dal reale titolare. Secondo l'opinione prevalente nella dottrina italiana tale fenomeno è riconducibile al regime della rappresentanza [89], talora in via diretta [90], talaltra in via di applicazione analogica [91].

Un'obiezione che viene talora mossa a tale impostazione prende spunto dall'assenza, nella fattispecie, della *contemplatio domini*: il terzo non ha modo di rendersi conto di interagire con un soggetto diverso dal titolare del certificato, onde non ricorrerebbe un tratto essenziale del fenomeno rappresentativo. Tale approccio ha però il difetto di realizzare un indebito rovesciamento di prospettiva. La *contemplatio domini* (come appare soprattutto, in modo articolato e rivelatore, del §164 BGB) ha la funzione di rendere palese al terzo che il vincolo giuridico che si va a creare non impegnerà il

[88] Articoli 27-bis e 28-bis del TU455/2000, già citato.

[89] Un punto di riferimento talora utile è rappresentato dalla figura del biancosegno, specie per quanto concerne i rapporti con i terzi, ma discorrere in termini di biancosegno da un lato poco dice sulla natura del rapporto intercorrente tra titolare del dispositivo e soggetto agente, e d'altro lato pone in ombra il fatto che nel biancosegno ogni singola firma è apposta dal soggetto cui è il documento è imputabile, mentre con l'affidatario del dispositivo di firma può porre in essere un numero indefinito di firme: la differenza pare non meramente quantitativa.

[90] Sulle orme di W. FLUME (*Allgemeiner Teil des bürgerlichen Rechts*, II, Springer, Berlin et al. 1979, p. 776), M. MICCOLI, *Commercio telematico: una nuova realtà nel campo del diritto*, Milano, IPSOA 1998, p. 35; C.M. BIANCA, *I contratti digitali*, in *Studium Iuris*, 1998, p. 1038; l'argomento è stato pure trattato da U. BECHINI e M. MICCOLI, *La forma sine probatione*, in *Notariato*, 2002, p. 332.

[91] A.M. GAMBINO, voce *Firma Digitale*, in *Enciclopedia Giuridica Treccani*, Roma 1999, p. 8; R. ZAGAMI *Firma digitale e sicurezza giuridica*, cit, p. 278 ss. Si ritrova in una classica dottrina (P. GUIDI, *Teoria giuridica del documento*, Giuffrè, Milano 1950, p. 76) l'affermazione secondo cui la sottoscrizione operata dal mandatario vergando il nome del mandante fa sì che autore del documento debba essere considerato il mandante, ma che il documento stesso non potrà integrare gli estremi della scrittura privata mancando il requisito dell'autografia.

soggetto agente, ma il terzo rappresentato [92]. Se questo è esatto, rimarcare l'inesistenza della *contemplatio domini* non appare pertinente nella nostra ipotesi ove, ben al contrario, è il soggetto agente a restare occulto, ed il terzo entra il relazione giuridica proprio col soggetto di cui gli è nota l'identità.

La posizione più severa [93] si attiene invece, in stretta aderenza al dettato normativo, all'identità formale tra documento elettronico e tradizionale documento scritto, e non esita quindi a riconoscere nell'apposizione della firma digitale da parte di soggetto diverso dal titolare un puro e semplice falso. Quest'approccio necessita di ulteriore verifica. La soluzione deve essere ricercata non mediante l'applicazione diretta di istituti esistenti, ma attraverso il preventivo esame delle caratteristiche proprie della fattispecie, delle sue peculiarità rispetto alle più simili fattispecie espressamente regolate, e del contemperamento degli interessi tutelati. Rilevano in questi casi i principi generali dell'apparenza, della tutela dell'affidamento, della buona fede e della diligenza, ed è presumibile che la giurisprudenza farà ricorso a questi per fattispecie la cui differenza ontologica rispetto a quelle già regolate non consente applicazione estensiva o analogica [*94*].

In tale ottica, è legittimo chiedersi se possa davvero discorrersi di apocrifia in relazione ad una figura (la firma digitale apposta da terzi) che non include nel suo statuto ontologico (a differenza della firma autografa) alcuna traccia dell'intervento di soggetto diverso da quello cui la sottoscrizione è imputabile. A chi obietta che così facendo si commette l'errore concettuale di confondere il fatto in sé con la pratica

---

[92] La contemplatio domini serve appunto a superare la presunzione che chi tratta è anche colui che acquista i diritti ed assume le obbligazioni, e soddisfa l'esigenza di tutelare il terzo contraente in ordine alla persona che diviene sua controparte nel rapporto contrattuale. Questa esigenza di comunicare al terzo contraente l'alienità dell'interesse per il quale si detta regola viene assolta con la prescrizione della contemplatio domini, espressione puntuale di un più generale principio in materia denominato dalla dottrina tedesca Offenheitsgrundsatz. Ma quando sussistono altri elementi che in concreto assolvono la stessa funzione protettiva dell'affidamento del terzo contraente oppure quando, dato il tipo di interessi regolati, non sorge proprio la necessità di tale protezione, ci sembra che egualmente si raggiunga, oppure si renda superfluo perseguire, il fine per il quale la norma impone l'agire in nome altrui, subordinando a quest'ultimo il prodursi dell'efficacia diretta per l'interessato. In altre parole, se l'unico scoglio perché si produca un tale tipo di efficacia è costituito dall'esigenza di tutelare il terzo rendendolo edotto su quale sarà la sua controparte contrattuale, è chiaro che tale ostacolo viene di fatto rimosso quando, come è appunto nelle ipotesi ora in considerazione di negozio sotto nome altrui, il terzo contraente proprio con il titolare del nome intende vincolarsi … (G. PIAZZA, Negozio sotto nome altrui, in Enciclopedia del Diritto, XXVIII, Giuffrè, Milano 1978, p. 133).

[93] M. DOLZANI, Il regime delle responsabilità. Obblighi dei soggetti interessati e spunti per un inquadramento sistematico; in Firme Elettroniche: questioni ed esperienze di diritto privato, Collana Studi del Consiglio Nazionale del Notariato, Giuffrè, Milano 2003, pp 89 ss.

[94] In tal senso E.A. GAETE GONZÁLES, *Instrumento público electrónico*, Bosch, Barcelona, 2002 [2], p. 135. Non sono pochi, in effetti, gli snodi del sistema PKI che con ogni verosimiglianza richiederanno ulteriori riflessioni ed approfondimento per l'esatta loro qualificazione giuridica. Certificati e liste di revoca, in particolare, esplicano un'efficacia che trascende i rapporti interni tra certificatore e soggetto certificato, giacché le firme digitali hanno valore (erga omnes) solo laddove adeguatamente supportate da conformi riscontri su tali databases, reperibili online sui siti dei certificatori. Si potrebbe forse avanzare addirittura il dubbio d'essere dinanzi ad un sistema pubblicitario di nuovo tipo, assai particolare sia per la natura privatistica dei gestori che per la peculiare efficacia della pubblicità. In effetti il contenuto dei certificati e delle liste di revoca fa (letteralmente) la differenza tra una firma ed una non firma, e quindi tra un contratto perfezionato ed uno non perfezionato: il tutto prescindendo da una preventiva adesione al sistema da parte del terzo che voglia avvalersi del documento firmato. Sotto questo specifico angolo visuale la pubblicità posta in essere dai certificatori pare dunque capace di penetrare nel cuore del rapporto civilistico persino più di quanto sia concesso alla trascrizione immobiliare, venendo ad assomigliare più da presso alle figure di pubblicità costitutiva.

opportunità di fornirne prova, si replica come si collochi a livello sostanziale, e non processuale, la difficoltà di spiegare per quale via un elemento che non contribuisce alla formazione della fattispecie possa assumere una rilevanza strutturale tale da fondare, in caso di sua patologia, addirittura un giudizio di illiceità.

Su un punto però vi è generale consenso: l'affidamento del dispositivo di firma ad un terzo è sicuramente illecito laddove ciò tenda a realizzare una delega de facto di funzioni indelegabili sul piano sostanziale. Non sarà quindi in alcun modo ammissibile, almeno nell'ordinamento italiano, l'affidamento a terzi della smart card da parte del notaio o di altro pubblico ufficiale, e neppure da parte dell'amministratore di una società per adempimenti di sua inderogabile personale responsabilità.

5. La morte del titolare

Può ben darsi che gli eredi ignorino l'esistenza di un certificato di firma elettronica intestato al defunto, e non segnalino quindi la circostanza al certificatore [95]. Laddove l'uso del dispositivo continui anche dopo la morte del titolare, le firme così apposte difetteranno probabilmente di un qualsivoglia valore giuridico, ma di ciò i terzi non avranno modo alcuno di accorgersi, restando quindi indotti a fare pieno affidamento sui documenti in tal modo sottoscritti. Si può anche pensare di percorrere l'itinerario ricostruttivo opposto, magari ipotizzando che la rivelazione del PIN [96] da parte del defunto equivalga al conferimento di una forma peculiare di potere rappresentativo: in determinate contesti normativi (è il caso dell'ordinamento italiano, articolo 1396 del codice civile, secondo comma) ciò fa prevalere la tutela della buona fede del terzo. Ad analogo esito si può pervenire argomentando in termini più generali, considerando come la circolazione della firma del defunto dipenda eziologicamente dalla mancata conservazione del PIN da parte del defunto, e sia quindi a lui (*rectius*: al suo patrimonio) in ultima analisi riferibile.

Ma questo è ancora un classico esempio di coperta troppo corta: così ragionando si farebbe nuovamente luogo ad una semplice operazione di *risk allocation*, trasferendo sugli eredi il rischio connesso ad usi abusivi *post mortem* del dispositivo di firma, ma senza realmente fare i conti con la sostanza della questione, che consiste nella possibile circolazione di firme assolutamente indistinguibili da quelle autentiche benché apposte dopo la morte del titolare.

6.1. La Direttiva 93/1999

Il panorama della legislazione italiana si è andato ulteriormente articolando per effetto dell'adeguamento alla già citata Direttiva Europea 93/1999. Questo testo, a differenza della previgente legislazione italiana, non contempla una figura unitaria e standardizzata, ma prevede una sorta di *continuum*, capace di accogliere un ventaglio

[95] E' significativo il confronto con l'attenzione del legislatore italiano del 1913, che evidentemente aveva un'idea un poco più precisa di quanto delicati siano i meccanismi per la produzione di documenti idonei a formare piena prova. L'articolo 38 della Legge Notarile impone infatti sia agli Ufficiali dello Stato Civile che agli eredi del notaro un obbligo di immediata comunicazione al Consiglio Notarile. L'attuale firma digitale del notaro certificata dal Consiglio Nazionale del Notariato italiano è immediatamente revocata a cura del Presidente Distrettuale in occasione della cessazione dalle funzioni, qualunque ne sia la causa.

[96] Qualora il defunto abbia portato il PIN con sé nella tomba, non si pone evidentemente problema alcuno, giacché il dispositivo di firma sarà inutilizzabile.

indefinito di tipologie. Al vertice *la firma elettronica avanzata* basata su un *certificato qualificato* rilasciato da un *certificatore accreditato* e creata mediante un dispositivo per la creazione di una *firma sicura*: corrisponde sostanzialmente alla firma digitale italiana. Al di sotto, la direttiva dà spazio a qualunque figura di firma elettronica, di cui dà la seguente definizione: *dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione*. Descrizione oltremodo vaga, che abbraccia anche tecnologie dai contenuti di sicurezza molto limitati, ma anche accorgimenti totalmente privi di qualunque connotato di sicurezza: persino una semplice immagine scannerizzata della firma autografa, che chiunque può procurarsi con straordinaria facilità. Forse persino un SMS o la semplice digitazione di un nome in calce ad una email [97].

L'evoluzione è in qualche modo fisiologica. La legislazione italiana del 1997, che come già ricordato era tra le prime al mondo, si poneva l'obiettivo di rendere quanto più accettabile possibile la dirompente novità del documento *paperless* a validità giuridica: a tal fine l'ovvia strategia era circondarsi dei migliori accorgimenti di sicurezza disponibili. Si aggiunga poi, come esposto più sopra, che le tecnologie digitali erano viste innanzitutto come uno strumento per lo snellimento della Pubblica Amministrazione: questo è un settore dove non si possono fare troppi sconti sul piano della certezza documentale e, nel contempo, occorre pure vincere resistenze e conservatorismi d'ogni specie. Tutto cospirava quindi verso un approccio estremamente prudente. La direttiva si muove invece a più ampio spettro. Da un lato non disconosce le peculiari esigenze legate all'uso della firma digitale in campo pubblico, sancendo anzi il diritto degli Stati di adottare a tal proposito tutti gli accorgimenti che loro paiano opportuni, purché *obiettivi, trasparenti, proporzionati e non discriminatori* (art. 3 della Direttiva). D'altro lato riconosce cittadinanza alle forme minori di firma elettronica richieste dalla pratica commerciale.

Queste ultime però non possono ovviamente che godere di uno *status* inferiore sotto il profilo probatorio. L'approccio della Direttiva (articolo 5), è liberale ma senza eccessi. La firma digitale possiede i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei, ed è ammessa come prova in giudizio. Ciò coincide tra l'altro con la previgente legislazione italiana e non pone speciali problemi. Per le firme elettroniche "minori" si è previsto invece quanto segue: *gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:*

- in forma elettronica, o
- non basata su un certificato qualificato, o
- non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero
- *non creata da un dispositivo per la creazione di una firma sicura.*

[97] L'ipotesi è stata affacciata in P. PICCOLI ed U. BECHINI, *Documento informatico, firme elettroniche e firma digitale,* in *I problemi Giuridici di Internet* (a cura di Emilio Tosi), tomo primo, Giuffré, Milano 2003, pagina 239 nota 107; nello stesso senso S. MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 101

I Paesi dell'Unione sono quindi tenuti a non adottare normative che discriminino in via pregiudiziale (si noti l'avverbio *unicamente*) le firme elettroniche non provviste di specifici attributi di sicurezza, e sin qui non sorgono speciali difficoltà.

La normativa europea non è dunque una vera e propria *thin law*, ma ha un approccio più articolato [98]: da un lato ha consacrato la massima libertà di scelta sul piano tecnologico, dall'altro ha confermato la firma digitale vera e propria come strumento principe per la produzione di documenti provvisti dello stesso valore giuridico di quelli cartacei [99].

6.2. Il D.Lgs. 10/2002

Il fatto è che in sede di attuazione della direttiva il legislatore delegato italiano si è spinto molto più innanzi, senza che la Direttiva lo richiedesse[100] né, quel che è peggio, che la legge delega lo autorizzasse: l'articolo 10 del già citato TU 445/2000 così recita: *Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.*

La firma elettronica leggera, qualunque firma elettronica, è dunque sufficiente ad integrare gli estremi della forma scritta, salvo che sul piano probatorio il documento così sottoscritto è liberamente apprezzabile dal giudice. Le applicazioni pratiche possono essere sconcertanti [101]: una firma elettronica semplice potrà essere utilizzata per sottoscrivere (validamente! [102]) una vendita immobiliare, ma il giudice potrà poi "liberamente valutare" l'attendibilità del documento.

La norma finisce così per attribuire l'efficacia del documento scritto ad entità che possiamo senz'altro definire intrinsecamente insicure [103], in quanto non posseggono le caratteristiche che inducono il legislatore a richiedere la forma scritta a pena di nullità per negozi cui deve essere assicurata una tutela di più alto livello. Il documento cartaceo

---

[98] L'impostazione è peraltro condivisa anche da alcune legislazioni USA, come l'Illinois Electronic Commerce Security Act.

[99] Questo atteggiamento è criticato da C. SPYRELLI, Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication, in The Journal of Information, Law and Technology (JILT) 2002/2. L'Autrice reputa che il doppio binario europeo (firme digitali a valore giuridico assicurato, altre firme elettroniche a regime incerto) renda la libertà di scelta della tecnologia molto più teorica che negli USA, ove invece nessuna soluzione gode di uno status privilegiato. Non sembra però che questa situazione abbia finora favorito la diffusione della firma elettronica negli USA, che al contrario pare rallentata anche dalla perdurante totale incertezza sui possibili orientamenti di una corte americana chiamata a decidere in simili contesti. Sembra anzi azzeccata la feroce battuta di P. HOFFMAN (The pen is mightier than the electronic signature, in *Network World*, 24/7/00) secondo cui la legislazione statunitense pare perseguire una politica di tipo FEFL (*Full Employment For Lawyers*, piena occupazione per gli avvocati).

[100] Al punto da far seriamente prendere in considerazione l'idea che la normativa italiana costituisca tout court violazione della Direttiva europea.

[101] Tra le prime e più vigorose critiche quelle di M. CAMMARATA ed E. MACCARONE, *A chi conviene la certificazione insicura?*, in *Interlex*, 17/01/02, http://www.interlex.it/docdigit/recepiment2.htm

[102] La forma scritta è sufficiente, nell'ordinamento italiano, per un valido trasferimento immobiliare; l'autentica notarile (o l'atto pubblico) sono richiesti solo per la pubblicazione dell'atto nei registri immobiliari.

[103] Espressione tenuta a battesimo in Italia da M. CAMMARATA ed E. MACCARONE, *Il Governo cancella un vanto dell'Italia*, in *Interlex*, 10/01/02, http://www.interlex.it/docdigit/recepimento.htm.

deve il suo tradizionale status ad alcune ben evidenti proprietà: la conoscibilità senza necessità dell'intermediazione di uno strumento meccanico o tecnologico, la durevolezza nel tempo, la rilevabilità delle alterazioni, e la possibilità di imputarne la paternità al soggetto che attraverso la sottoscrizione lo abbia riconosciuto proprio. Il documento informatico munito di firma elettronica semplice, come definita dalla direttiva europea, non soddisfa alcuno di questi requisiti: richiede un mezzo tecnico per la sua conoscibilità, e non vi è alcuna garanzia di reperibilità nel tempo di tale strumento, non essendo necessaria l'utilizzazione di alcuno strumento standard; non ne è garantita le durevolezza, né tanto meno il tempo della formazione; non è imputabile con certezza ad alcun soggetto. Ciò non significa che singoli documenti o classi di documenti non rispondano ad alcuni od anche a tutti tali requisiti; semplicemente ciò non è prescritto, e sembra eccessiva la tutela riconosciuta dalla norma ad un documento che non offre alcuna garanzia [104].

Di tutto questo pare in qualche modo cosciente il legislatore italiano quando rimette al giudice il libero apprezzamento dell'attendibilità del documento. Ma la soluzione è ben lungi dal risultare soddisfacente, venendo anzi a spezzare il tradizionale interagire e reciproco completamento tra prescrizioni operanti sul piano della forma e le regole che compongono il sistema probatorio. A volerla risolvere con un calembour[105], sembra insomma che nel nostro ordinamento sia stata introdotta, quasi a contraltare (involontariamente) ironico della forma *ad probationem*, un'inedita forma *sine probatione*, che contraddice il comune insegnamento secondo cui la forma *ad substantiam* non è mezzo di prova [106], ma è anche (e forse: soprattutto) predisposizione del mezzo di prova. La fisiologia giuridica della firma elettronica leggera viene dunque ad assomigliare, in modo assai rivelatore, al panorama che si riscontra tradizionalmente in caso di perdita o distruzione della scrittura, in cui il requisito sostanziale della forma è reputato storicamente soddisfatto, salve le incertezze sul piano probatorio.

Constatare come il regime ordinario di queste figure corrisponda a quanto sino ad oggi ha avuto cittadinanza nell'ordinamento solo come ipotesi patologica, sarebbe forse già di per sé un commento sufficiente. Ma v'è di più. Appare insopportabilmente contraddittorio che uno strumento destinato a documentare (e quindi: a predisporre la prova di) operazioni di commercio elettronico, per le quali non è mai stata richiesta la forma scritta, fornisca un astratto quanto inutile status di forma scritta, e nessuna certezza sul piano probatorio.

7. La firma digitale affonda?

Ancora verso la fine degli anni Novanta, era opinione diffusa quella secondo cui le firme digitali avrebbero rappresentato uno strumento insostituibile per il decollo del commercio elettronico. Tale prognosi non ha trovato conferma nell'esperienza pratica degli anni recenti, né in Italia né a livello internazionale.

---

[104] E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, p. 1133. Il saggio è apparso in AAVV, Diritto dei consumatori e nuove tecnologie, Giappichelli, Torino 2003; le pagine si riferiscono però all'anteprima apparsa su *Vita Notarile*, 2003/2.

[105] Si ripropone qui una formula presentata in U. BECHINI e M. MICCOLI, *La forma sine probatione* in *Notariato*, 2002, p. 329.

[106] N. IRTI, Il contratto tra faciendum e factum, Rassegna di diritto civile, 1984, p. 938; anche in Idola Libertatis, Milano 1985, ed ora in Studi sul formalismo negoziale, Milano 1997, p. 120.

Vi è consenso sulle ragioni di tale fenomeno [107]. L'ambito operativo in cui ci si attendeva che la firma digitale potesse andarsi a collocare ha subito una duplice erosione: semplificando, potremmo dire che il tradimento delle aspettative è venuto sia dall'alto che dal basso.

Il mondo del business ha dimostrato di non averne grande necessità. I rapporti d'affari, specie ad alto livello, si articolano lungo tutta una serie di occasioni di contatto (incontri diretti, telefonate, lettere, dispacci fax, videoconferenze), e si appoggiano su una rete di collaudate relazioni, dirette ed indirette, che rendono generalmente superflua una fase di reciproca identificazione formale delle parti contraenti, del tipo garantito dalla firma digitale.

Non miglior sorte la firma digitale ha incontrato nel mondo del commercio elettronico [108] che, da parte sua, ha a propria disposizione strumenti informatici assai più semplici [109], che non pongono a carico dell'utente una fastidiosa fase di registrazione e

---

[107] Si veda l'acuta analisi di J.K. WINN, *The Emperor's New Clothes*, cit. Il riferimento alla celebre favola di Andersen serve alla studiosa statunitense (docente di Internet Law a Berkeley e presso la Washington University di Seattle), non solo per annunciare che il Re (la firma digitale) è nudo, ma anche per insinuare un parallelo tra il Re, che spende grandi somme per abiti inesistenti, e le aziende che hanno creato costose infrastrutture di firma digitale: *many years and untold millions of dollars later, no major market participants have been able to promote widespread use of that technology based on that standard* (molti anni ed imprecisati milioni di dollari più tardi, nessuno dei principali operatori è stato in grado di promuovere un diffuso impiego di tale tecnologia). Ed ancora: *there is mounting evidence that trying to use asymmetric cryptography as a signature on a contract is like trying to fit a square peg into a round hole, and the effort to get that square peg into that round hole has created a phenomenal sink hole into which countless individuals and organisations have poured vast resources with few tangible payoffs in sight* (è sempre più evidente che cercare di usare la tecnologia a chiavi asimmetriche per firmare contratti è come cercare di infilare un piolo quadrato in un foro tondo; i tentativi in tal senso hanno creato un fenomenale buco nero in cui innumerevoli individui ed organizzazioni hanno gettato vaste risorse, con pochi ritorni tangibili in vista). Per analoghe considerazioni ci sia consentito rinviare pure ad U. BECHINI, *Quando la smart card diventa un souvenir*, in *Interlex* (www.interlex.it), 21/9/01; sulla stessa linea H. MORIN, *Pourquoi la signature électronique reste lettre morte*, in *Le Monde*, 23/5/03.

[108] Molto lucidamente, M. CAMMARATA e E. MACCARONE, *Introduzione alla firma digitale*, cit. (7 / *Serve anche al commercio elettronico?*), in *Interlex* (www.interlex.it) 16/12/99. Nello stesso senso il successivo contributo di C. ELLISON e B. SCHNEIER *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*, (in *Computer Security Journal*, v 16, n 1, 2000, p. 1): *Open any article on PKI in the popular or technical press and you're likely to find the statement that a PKI is desperately needed for e-commerce to flourish. This statement is patently false. E-commerce is already flourishing, and there is no such PKI. Web sites are happy to take your order, whether or not you have a certificate. Still, as with many other false statements, there is a related true statement: commercial PKI desperately needs e-commerce in order to flourish*. (Prendete qualunque articolo in materia di PKI, sulla stampa specializzata o meno, e leggerete che il commercio elettronico ha disperatamente bisogno delle PKI per decollare. Ciò è palesemente falso. Il commercio elettronico si sta già sviluppando senza nessuna PKI. I siti web sono ben felici di accettare il vostro ordine, che voi abbiate o meno un certificato. Tuttavia, come molte bugie, ha una verità collegata: le aziende che vendono servizi di PKI hanno disperatamente bisogno del commercio elettronico per decollare. Si veda da ultimo M. CAMMARATA ed E. MACCARONE, *La firma digitale sicura*, Giuffrè, Milano 2003, p. 229.

[109] In primis lo SSL. Tale sistema, sviluppato da Netscape, funziona nel modo seguente. Il server (che tipicamente apparterrà al commerciante online) con cui l'utente è in collegamento comunica la propria chiave pubblica al computer del utente; il software si occupa di verificare presso una Certification Authority che la chiave pubblica sia realmente quella dell'interlocutore desiderato. Il computer dell'utente genera quindi una chiave di tipo simmetrico, la cripta usando la chiave pubblica del server e la invia a quest'ultimo. Solo il server prescelto ed identificato potrà leggerla, perché solo quel server possiede la corrispondente chiave privata. Un terzo può certamente intercettare il messaggio, ma non saprebbe che farsene; laddove cercasse di ingannare il software dell'utente inviandogli la propria chiave pubblica, sarebbe smascherato in fase di verifica presso la Certification Authority. Server ed utente, che a questo

certificazione [110]. E' ben vero che tali sistemi non offrono il medesimo livello di sicurezza della firma digitale, ma limitazioni tecniche che in altri contesti potrebbero risultare insopportabili, nel mondo dell'*e-commerce* sono facilmente gestibili [111]. Nella stragrande maggioranza dei casi, è sufficiente l'intervento di un terzo, il gestore della carta di credito: questi garantisce il pagamento, assumendosi nei confronti del venditore tutti i rischi di insolvenza delle transazioni. Ciò è reso possibile da due fattori concomitanti: l'ammontare di ogni singola transazione è mediamente basso ed il numero di esse è notevolmente alto. Anche laddove un non trascurabile numero di esse non vada a buon fine, il gestore della carta di credito può quindi sopportare l'onere del rimborso del prezzo non corrisposto dal cliente finale. Uno scenario comunque enormemente più attraente, per un operatore commerciale, rispetto ad infrastrutture magari supersicure ma cui pochissimi consumatori accederebbero a causa delle inevitabili complicazioni.

Va poi osservato che interi settori hanno proseguito nell'utilizzo di tecnologie specifiche: è il caso di tutti i sistemi adoperati nel mondo bancario, ad esempio per le comunicazioni tra istituti oppure per la gestione remota degli sportelli ATM (in Italia più noti col nome commerciale di Bancomat). In generale, tutto il settore finanziario non ha manifestato grande attenzione per la firma digitale, con ciò facendo mancare un trampolino di importanza strategica. Non che in tale campo non si impieghino strutture di tipo PKI [112]: se ne ritrovano anzi ottimi esempi come Identrus [113] e SET [114]. Si tratta però di infrastrutture operanti solo all'interno di una platea di interlocutori predefiniti [115]: cosa ben diversa [116] dalla firma digitale a valore legale *erga omnes*, che consente a

---

punto condividono segretamente una loro esclusiva chiave simmetrica, possono utilizzarla per la successiva comunicazione. Questa procedura, oltre a consentire intrinsecamente una maggior velocità, data la maggior leggerezza computazionale di tali algoritmi, non richiede la generazione di una coppia di chiavi asimmetriche da parte di ciascun utente. Da notare infine che è l'utente ad identificare il server con cui desidera comunicare, non viceversa. Tutto ciò che SSL può fare, in buona sostanza, è assicurare l'utente di essere davvero in comunicazione con il server da lui prescelto, e che i dati in transito non possono agevolmente essere letti da terzi. Le lacune sono evidenti: il server non ha affatto la certezza di essere in contatto con quel determinato utente, e non vi è alcuna forma di documentazione obiettiva del contenuto delle comunicazioni scambiate. Il sistema quindi non offre molto: quanto basta però a convincere l'utente non troppo prevenuto a digitare con serenità, ad esempio, il numero della propria carta di credito, nella ragionevole certezza che solo il computer del fornitore da lui prescelto potrà leggerlo. Il tutto senza porre a carico dell'utente né la previa iscrizione presso sistemi di certificazione né operazioni complesse sul piano informatico, in quanto la gestione del protocollo SSL è svolta dal browser in maniera assolutamente invisibile. Come è stato un po' crudelmente osservato da J. K. WINN, *op.ult. cit.*, il travolgente successo del sistema SSL deriva dal fatto che *non è* una firma.

[110] L'emissione di un certificato di firma digitale non è operazione lunga o costosa in termini assoluti, ma resta poco verosimile imporla a chi voglia fare soltanto un poco di shopping online.

[111] Per una contrapposizione tra *Formalistic model* e *Risk-Based Model*, si veda W. FORD e M.S. BAUM, *Secure Electronic Commerce*, cit., p. 67.

[112] Vedasi al § 2.1.2.

[113] Che fa riferimento ad un pool di banche di tutto il mondo, molte delle quali europee.

[114] Sistema destinato alla gestione dei pagamenti via carta di credito, creato da Visa e MasterCard.

[115] In genere in ambito cosiddetto B2B (*business to business*), espressione invalsa nel gergo Internet in contrapposto a B2C (*business to consumer*). Secondo M. MEEHAN, *Energy industry to adopt digital signatures*, in *Computerworld*, 3/5/02, la più importante applicazione di strutture PKI negli USA era all'epoca un sistema di trading online dell'energia, cui partecipa ad esempio UBS Warburg Energy, che ha rilevato l'attività di Enron. I certificati costavano 175 dollari l'anno per ogni dipendente abilitato al trading.

chiunque di accertare la provenienza e l'integrità di qualunque file digitalmente sottoscritto da chiunque altro, anche in assenza di alcun previo rapporto o dell'appartenenza ad un unico sistema od organizzazione.

Il *De profundis* per la firma digitale è però a dir poco prematuro. Sul piano degli impieghi commerciali il panorama non pare roseo, ma l'esperienza ha insegnato quanto sia imprudente formulare prognosi. Comunque sia di ciò, vi è un settore in cui la firma digitale appare al momento uno strumento insostituibile, ed è quello dei rapporti in cui è comunque coinvolta la Pubblica Amministrazione. In tale contesto non si può fare a meno di una già menzionata caratteristica che solo la firma digitale pare in grado di offrire, e cioè la possibilità di accertarne provenienza ed integrità, sempre, ovunque, e da parte di chiunque; per converso, i modelli operativi alternativi, più sopra ricordati, che paiono al momento aver tenuto il mondo dell'impresa lontano dalla firma digitale, obbediscono a logiche e dinamiche puramente commerciali e non sono in alcun modo trasferibili al settore pubblico.

Non è un caso che diverse legislazioni in materia di firma digitale abbiano preso le mosse proprio dalle esigenze di snellimento del settore pubblico: quella italiana e quella californiana [117], ad esempio. Un po' dappertutto il maggior interesse per i sistemi di firma digitale è a livello governativo [118], e non nel mondo dell'impresa.

Questa circostanza ha potenzialmente rilevanza strategica. In molti Paesi l'intreccio tra funzioni pubbliche ed attività economiche private è enormemente più fitto rispetto a quanto accada negli USA, ove normalmente i pubblici uffici non si occupano neppure di certificare chi sia l'attuale legale rappresentante di una società. L'affermarsi della firma digitale in campo pubblico avrebbe quindi un impatto globalmente maggiore, e per così dire più pervasivo, rispetto a quanto potrebbe accadere Oltreoceano. Non vi sarebbe insomma motivo di stupore se nel giro di qualche anno si vedesse la firma digitale prendere piede in Europa, in America Latina ed in Estremo Oriente in modo più robusto rispetto agli stessi Stati Uniti.

L'approccio *technology-neutral* prediletto dagli statunitensi porta inoltre con sé il suo bagaglio di rischi aggiuntivi, anche nel settore pubblico. Non potendosi pretendere che gli uffici pubblici accettino una varietà indefinita di sistemi di autenticazione e firma, il rischio [119] è che ogni amministrazione prescelga un sistema proprio, creando una pletora di circuiti reciprocamente incompatibili [120]. Il pubblico non professionale,

---

[116] Dal punto di vista giuridico almeno: dal punto di vista tecnico può non esserci alcuna differenza. Fenomeno non nuovo: anche se una Intranet usa tutta la tecnologia di Internet, non per questo *è* Internet.

[117] La Sezione 16.5 del California Government Code inizia con queste parole: In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section (In ogni comunicazione scritta con un pubblico ufficio, come definito alla Sezione 811.2, in cui una firma è richiesta od utilizzata, ogni parte della comunicazione può apporre una firma digitale conforme alle previsioni di questa sezione).

[118] Gli esempi potrebbero essere molti: negli Stati Uniti il maggior promotore dell'uso della firma digitale è il governo federale nell''ambito dell'attuazione del cosiddetto Government Paperwork Elimination Act; in Italia è a regime l'operazione forse più ampia in assoluta, la trasmissione dei dati al Registro delle Imprese; in Germania il governo federale ha deciso nel gennaio 2002 di dotare di firma elettronica ogni dipendente federale entro il 2005 (CNN 21/1/02).

[119] R.A. WITTIE e J.K. WINN, Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA, in The Business Lawyer, 2000, p. 293.

[120] Potrebbe persino ripetersi quanto è accaduto nel campo della telefonia mobile: il sistema unico paneuropeo GSM si è rapidamente diffuso in tutto il mondo, mentre il mercato USA, spezzettato tra molti

che non ha occasioni frequenti di contatto con una determinata amministrazione, rischia di essere assai meno incentivato all'uso delle tecnologie digitali di quanto potrebbe essere in un contesto in cui una (ed una sola) smart card è utilizzabile in una molteplicità di occasioni.

standard incompatibili tra loro, è rimasto visibilmente più arretrato, ed alcuni operatori hanno addirittura trovato conveniente importare il sistema europeo. E' curioso leggere, una volta tanto, i meravigliati reportages dei media americani sull'avanzata delle tecnologie wireless europee: ad esempio J. MARKOFF, *Americans don't get the message*, in *International Herald Tribune* 3/9/02 (ripreso con minime variazioni da *U.S. Cellphone Users Don't Seem to Get Message About Messaging*, in *The New York Times*, 2/9/02).

CAPITOLO III

LA FIRMA DIGITALE APPLICATA ALLA FUNZIONE NOTARILE

SOMMARIO.1. Aree di impiego; 2. Riconoscibilità della funzione; *2.1* - Riconoscibilità (segue): le Certification Authorities notarili*;* 3. La durata del documento informatico; 3.1 - La verificabilità nel tempo; 4. La firma digitale: un pericolo per il notariato?

1. Aree di impiego

Ad una prima analisi, non è dato riscontrare incompatibilità di fondo tra funzione notarile ed impiego della firma digitale. Il cuore della missione del notaio risiede nell'attività di consiglio ed assistenza che conduce alla redazione dell'atto, ed alla produzione di un documento provvisto di adeguata forza probatoria. In questo non vi è nulla che renda preferibile l'utilizzo di un supporto di tipo cartaceo rispetto alle forme di documentazione elettronica che abbiamo esaminato. L'atto notarile è tale poiché è firmato da un notaio, non in quanto è redatto su carta[121].

Sotto più di un profilo, l'intervento notarile appare anzi integrarsi perfettamente con l'impiego di queste tecnologie. Si è notato a più riprese come la firma digitale offra un elevatissimo livello di sicurezza a condizione che il suo impiego sia circondato da specifiche cautele ed attenzioni che il notaio, professionista della documentazione, può certamente provvedere meglio di chiunque altro, dotandosi dell'aggiornamento che il caso richiede. L'intervento del notaio nel mondo della documentazione in forma elettronica consente inoltre di unire alle doti intrinseche del documento elettronico, tra cui spicca l'enorme facilità di trasmissione a distanza, la valenza giuridica privilegiata del documento notarile.

Va però d'altra parte pure osservato che l'esigenza di procedere ad una documentazione in forma elettronica *ab initio* non appare una priorità della pratica notarile contemporanea[122]. La necessità di un'indagine personale della volontà delle parti, ad opera del notaio, rende sostanzialmente ineliminabile, almeno al momento, la presenza fisica delle parti dinanzi al notaio. Normalmente non vi sarà dunque alcuna particolare ragione per optare per la redazione di un originale in forma digitale; probabilmente l'originale cartaceo si farà anzi a lungo preferire, soprattutto per la facilità di raccolta delle sottoscrizioni e la collaudata conservabilità nel tempo.

Al momento, sembra quindi di poter affermare che la firma digitale non interesserà in modo massiccio la formazione della documentazione notarile originale, almeno nell'immediato futuro. Ciò non toglie che l'impiego potrà essere imponente, come lo è già in Italia, in alcuni importanti ambiti. I principali tra questi appaiono essere la produzione di:

---

[121] Prendo in prestito l'espressione dalla brillantissima relazione di B. REYNIS, *Signature électronique et acte authentique, le devoir d'inventer*, relazione al XXII ongresso annuale del Comitato Francoitaliano del Notariato Ligure e Provenzale sul tema *Atti autentici in Europa e firma elettronica* (Genova 21/22/23 settembre 2001) http://web.tiscali.it/conoge/italofrancese/ge_re.htm (anche in JCP éd. N, 12 Oct. 2001, p.1494) .

[122] S. CHIBBARO, Le problematiche giuridiche delle prime applicazioni, in AA. VV., Firme Elettroniche: questioni ed esperienze di diritto privato, cit., pp 109 ss.

copie autentiche, specialmente se destinate a pubblici uffici, per formalità di pubblicazione o d'altro tipo;

procure ed altri documenti abilitativi, destinati soprattutto alla trasmissione ad altri notai, del medesimo o di altro Paese;

dichiarazioni di volontà dirette ad integrarsi con altre dichiarazioni rese dinanzi a notai di luoghi diversi, onde formare atti *inter absentes*.

Per svolgere adeguatamente questi compiti, e gli altri che la prassi saprà affidargli, occorre che il notaio abbia a sua disposizione strumenti che consentano di dotare il documento elettronico da lui prodotto di tutti i tradizionali attributi del documento notarile. Il documento provvisto di firma digitale possiede per qualità intrinseca alcuni tra questi. Altri presentano profili di maggiori criticità, e tre in particolare meritano un approfondimento:

la riconoscibilità della funzione;

la durata del documento informatico;

la verificabilità nel tempo.

Prima di entrare brevemente nel merito di ciascuno di tali punti, un'osservazione di carattere più generale. Nella letteratura italiana ha avuto luogo, in epoca immediatamente successiva all'apparizione della legislazione sulla firma digitale, un dettagliato dibattito sulla possibilità di formare originali notarili sottoscritti digitalmente. Larga parte di tale dibattito si articolava intorno a peculiarità specifiche del sistema normativo italiano, di scarso interesse in questa sede [123], ma una constatazione di maggior respiro[124] merita certamente di essere qui riproposta. Come si vedrà meglio più innanzi, il documento informatico, per sua intrinseca natura, si presenta assai carente sotto almeno uno dei ricordati aspetti: la durata nel tempo. Il conflitto con una delle caratteristiche fondamentali della documentazione notarile non potrebbe essere più netto. La soluzione del problema è certamente possibile ma si tratta di questione complessa, e comporta l'adozione di scelte discrezionali tutt'altro che ovvie e scontate. Per questa ragione, strutturale e non incidentale, pare impensabile passare alla produzione di originali notarili in forma digitale in assenza di un preciso quadro di riferimento normativo che stabilisca forme e modalità della conservazione. La durata nel tempo dell'originale notarile è argomento sul quale non è ammessa approssimazione alcuna.

2. Riconoscibilità della funzione

La firma digitale assicura la riferibilità di un documento da una determinata chiave di firma. Abbiamo osservato come questo non equivalga all'accertamento della provenienza del documento da una determinata persona fisica, per una serie di precise ragioni. Ma l'analisi di tali ragioni consente di affermare che quando tali sistemi sono oggetto di un impiego in ambito professionale da parte di soggetti dotati di specifica qualificazione e di elevatissima responsabilizzazione, le avanzate riserve perdono significato.

[123] Anche se in qualche caso attirano tuttora l'attenzione su questioni che meritano con ogni probabilità soluzione normativa. Come si allega, ad esempio, una procura in forma digitale ad un originale cartaceo? Si veda anche G. PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile* in *Notariato*, 1997, p. 567

[124] Su cui S. CHIBBARO, Le problematiche giuridiche delle prime applicazioni, in AA. VV. Firme Elettroniche: questioni ed esperienze di diritto privato, cit., p 109.

Altra e distinta questione è la riconoscibilità della funzione. Un conto è accertare che una determinata firma appartiene a Tizio: altro affare incorporare nella firma digitale accorgimenti opportuni a far sì che chi procede alla verifica della firma possa contestualmente assicurarsi che Tizio è notaio, regolarmente in esercizio e nella pienezza delle sue funzioni.

Si obietta frequentemente che così ragionando si pretende immotivatamente dalla firma digitale l'obbedienza a parametri di sicurezza superiori a quello offerti dalla carta. Chi mai esegue nel mondo cartaceo una verifica del tipo appena descritto?

Vero, ma non immotivato. Non bisogna dimenticare che nella firma digitale una sequenza di bit deve rimpiazzare, da sola, una pluralità di elementi, che nel supporto cartaceo concorrono a formare un quadro di certezza affinato e sperimentato nel corso dei secoli. Come è stato scritto: *I documenti cartacei sottoscritti posseggono attributi intrinseci di sicurezza che sono assenti nelle documentazioni informatiche. Tra questi l'ineliminabilità dell'inchiostro assorbito dalle fibre della carta, l'inimitabilità di ogni procedimento di stampa (ad esempio per la carta intestata), le filigrane, i parametri biometrici della firma (pressione, forma, direzione della penna sono caratteristici dell'autore della firma) la disponibilità di timestamp (come i timbri postali), e la visibilità di modifiche, interlinee e cancellature* [125]. Sono molti, in altri termini, gli indizi fisici dell'autenticità di un documento notarile su carta, ben percepibili da un operatore manuale mediamente esperto. Nulla di tutto ciò in un documento firmato digitalmente.

E non è tutto. Un uso efficiente della firma digitale si realizza nell'ambito di procedure altamente automatizzate, con un intervento umano limitatissimo quando non assente. Già oggi il Catasto italiano procede alla cosiddetta voltura, il mutamento dell'intestazione degli immobili, senza alcun intervento umano, sulla sola base di un documento digitalmente sottoscritto dal notaio. Tale modo di procedere risulta altamente gradito sia all'Amministrazione pubblica, che vede abbattersi in modo spettacolare i costi di personale, sia al Notariato, che nell'acquisizione automatica, non filtrata, dei dati forniti dai singoli notai, vede un riconoscimento della qualità della sua funzione. Ma è impensabile attivare simili procedure in assenza di un meccanismo che dia certezza della provenienza dei dati da un soggetto che riveste la qualifica di notaio.

2.1 - Riconoscibilità (segue): le Certification Authorities notarili

Si è già accennato in precedenza [126] che il tema delle funzioni costituisce uno dei punti nodali per la esercizio della firma digitale in un ambito di applicazioni volte principalmente all'interazione con la Pubblica Amministrazione.

Già la definizione che spesso si utilizza, ed alternativa a quella più propriamente tecnica di enunciazione dei ruoli, di enunciazione funzioni, qualifiche, poteri, è locuzione volutamente ampia ed omnicomprensiva, non corrispondente in sé ad una singola categoria dogmatica, ma ad una serie di istituti e categorie che condividono la caratteristica del necessario conferimento di un potere da parte di un soggetto, terzo rispetto al soggetto agente, per la validità od efficacia dell'atto posto in essere. Riportando la definizione a categorie generali, essa ricomprende: la sostituzione

[125] Non si tratta del frutto della penna d'oca di un notaio *d'antan*: il brano è tratto dalla seconda edizione (2001) di *Secure Electronic Commerce, Prentice Hall* (Upper Saddle River, New Jersey), pagina 5. Autori Warwick Ford e Michael S. Baum: si tratta dei due vicepresidenti di VeriSign, ossia del primo fornitore al moCndo di servizi di firma digitale. Sul punto cfr. infra nel testo

[126] Cfr. supra, § 1.3.

nell'attività giuridica[127], la delegazione amministrativa, l'esercizio di pubbliche funzioni, l'esercizio di attività soggette ad autorizzazioni ed abilitazioni (quali le libere professioni).

Le peculiarità del tema devono essere affrontate sia dal punto di vista dell'ordinamento giuridico generale, nazionale ed internazionale, sia dal punto di vista della specifica disciplina di settore.

Abbiamo già chiarito che il documento informatico, e la firma digitale che ne costituisce metodo primario di imputazione, devono essere trattati in primo luogo dal punto di vista della realtà fenomenica, per chiarire in che misura le differenze ontologiche[128] del documento informatico, rispetto al documento tradizionale, incidano sulla qualificazione delle fattispecie giuridiche che lo riguardano. E' indubitabile infatti, da un punto di vista generale, che, se tra documento tradizionale e documento informatico non mutano le posizioni tutelate dall'ordinamento, mutano invece le caratteristiche del mezzo utilizzato, in modo che non può essere pregiudizialmente considerato neutro, e quindi giuridicamente irrilevante. Non può infatti ritenersi che la semplice equiparazione del documento informatico a quello cartaceo, e della firma digitale (e poi in parte di quella elettronica) a quella autografa, costituisca per l'interprete una dispensa dall'indagine sulle fattispecie[129].

Occorre poi considerare che la firma digitale stravolge un criterio di imputazione del documento[130] cartaceo[131], vecchio di millenni ed accettato socialmente fino al punto di non necessitare di esplicite definizioni e riconoscimenti normativi,[132]. E' per tali

---

[127] Si riprende la locuzione dal F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1983, pag. 266, che include nella stessa tutte le ipotesi di sostituzione astrattamente ipotizzabili, e quindi la rappresentanza volontaria, legale, ed organica, i fenomeni gestori, in presenza di autorizzazione.

[128] Quest'aspetto è esattamente colto da G. FINOCCHIARO,*La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in Comm. C.c. Scialoja-Branca a cura di Galgano, Bologna, 2000, pag. 1 ss., ed ancora in *Firma digitale e firma elettroniche. Il quadro normativo italiano dopo il d. legisl. 10/2002*, in Contratto e Impresa, 2002, pag. 853 ss. e, specificamente, pag. 854. L'Autore tuttavia giunge a conclusioni non condivisibili in materia di prova, su cui infra cap. II. Ci si permetta di rinviare anche a E. SANTANGELO M. NASTRI, *Firme elettroniche e sigilli informatici*, anticipato in Vita Notarile, 2/2002 pag. 1124, ed ora in AA.VV. (A CURA DI F. BOCCHINI) *Diritto dei consumatori e nuove tecnologie*, Torino, 2003, pag. 237 ss.

[129] Non sembra tuttavia che tale aspetto del problema sia stato sinora particolarmente presente alla dottrina. Da ultimo A.PIZZOFERRATO, *La "nuova" firma digitale nell'esperienza giuridica italiana*, in Contratto e Impresa Europa, 2002, pag. 78 afferma che ci si trova di fronte "ad un assetto normativo estremamente lineare e pulito che la dottrina ha caricato, naturalmente la critica non è generalizzabile, di una serie di falsi problemi."

[130] Per A. GRAZIOSI, *Premessa ad una teoria probatoria del documento informatico*, in Riv.Trim.di Dir. e Proc. Civ., *1998*, pag. 503, "Sul piano sostanziale la sottoscrizione può essere qualificata come un'autonoma dichiarazione convenzionale, mediante la quale un determinato soggetto si assume la paternità della dichiarazione rappresentata nel documento in calce al quale scrive il proprio nome".

[131] L'accertamento della paternità del documento cartaceo è legato ad elementi che sono il più delle volte riferibili ad un segno fisico collegato all'identità biologica del soggetto agente. Sulla sottoscrizione e sulla sua riferibilità ad un dato biologico o somatico F. CARNELUTTI, *Studi sulla sottoscrizione*, in Riv. Dir. Comm. 1929, pag. 509 ss.; A. MORELLO, *Sottoscrizione*, in Nov. Dig.It., vol. XVII, Torino, 1970, pag. 1003 ss., R. ZAGAMI, *Firma digitale e sicurezza giuridica*, Padova, 2000, pag. 180.

[132] La conseguenza sul piano del diritto vigente di tale stato di cose è che la sottoscrizione autografa non è nemmeno definita in positivo dal nostro ordinamento giuridico, ma ne è semplicemente regolata l'efficacia (in particolare artt. 2702 ss. c.c.), come rilevato da R. ZAGAMI, op. cit. pag. 5;

ragioni che il notariato, che del documento scritto con fede privilegiata è da altrettanto tempo artefice e custode, ha la necessità di essere soggetto attivo di tale fenomeno.[133]

Nell'ambito del documento informatico è interesse della collettività un livello di sicurezza del commercio giuridico che sia pari (e possibilmente superiore) a quello fornito dal documento cartaceo. E' altrettanto importante che tale livello di sicurezza sia ottenuto senza rinunciare ai risultati già acquisiti in ambito tradizionale, ma adeguando gli strumenti utilizzati alle caratteristiche del nuovo mezzo. L'esperienza del notariato, tradizionale produttore di documenti con altissimo grado di sicurezza giuridica, costituisce un patrimonio peculiare, e non comune a tutti coloro che si avvicinano ora, da utenti o attori del settore, al documento informatico con rilevanza giuridica.

Il documento informatico pone le stesse problematiche di carattere logico-giuridico di qualunque altro tipo di documento, ed in particolare quelle della autenticità e della integrità. Le firme elettroniche, e tra queste quella digitale[134] in particolare, costituiscono mezzi normalmente sufficienti a risolvere tali problematiche, e come tali sono riconosciute dalla legislazione nazionale e comunitaria, pur con l'incerto trattamento dei fenomeni patologici, che ha portato a modifiche sostanziali della disciplina nell'arco di pochissimi anni[135], ed è sostanzialmente dovuto alla diversità intrinseca tra firma elettronica e modalità tradizionali di sottoscrizione.

E' preferibile precisare che, ai fini del presente lavoro, il documento viene in rilievo particolarmente dal punto di vista contenutistico, come risultato dell'attività di documentazione, e quindi come "cosa che fa conoscere un fatto"[136] o meglio, per ciò che interessa, come cosa rappresentativa di un atto giuridicamente rilevante. La consistenza fisica del documento[137], e la pretesa mancanza di consistenza fisica del documento informatico[138], non rilevano ai fini della sua qualificazione giuridica. Rileva

---

[133] La scelta del Consiglio Nazionale del Notariato di divenire Certificatore delle firme digitali dei notai italiani è quindi funzionale ad una politica di valorizzazione della funzione del notaio, e di difesa dell'atto notarile quale documento munito di efficacia giuridica privilegiata, in virtù del preventivo controllo esercitato dal notaio circa i suoi attori ed i suoi oggetti, e soprattutto circa la sua conformità all'ordinamento giuridico.

[134] Sulla distinzione tra firma elettronica, firma elettronica qualificata, firma digitale, cfr. G. FINOCCHIARO, Firma digitale e firma elettroniche, cit. *passim.*, U. BECHINI –M. MICCOLI – *Attuazione della direttiva europea sulla firma elettronica, ovvero la forma "sine probatione"* in Notariato, 3/2002, pag. 327 ss., e E. SANTANGELO –M. Nastri, *Firme elettroniche*, cit. pag. 1126 ss..

[135] cfr. art. 10 del D.P.R. 445/2000 nella versione originaria e nella novella di cui al D.Lgs. 10/2002 ed infra cap. II

[136] F. CARNELUTTI, *voce Documento (teoria moderna) in* Noviss.dig. it., VI, Torino, 1960, pag. 86.

[137] Sul concetto di documento, e sulla specificazione come modalità della sua creazione, F. CARNELUTTI, *La prova civile*, Milano, rist., 1992, pag. 97; G. BETTI, *Diritto Processuale Civile Italiano*, Roma, 1936, pag. 356, nt. 98; D. DI SABATO, *Il documento contrattuale*, Milano, 1998, pag. 2 ss.; N. IRTI, *Sul concetto giuridico di documento*, in Riv. Trim. dir. Proc. Civ., 1969, e più di recente in *Studi sul formalismo negoziale*, Padova, 1997, pag. 159 ss., e, sulla definizione dell'attività di documentazione, pag. 175 ove l'Autore fornisce questa definizione:"*Il fare, onde la cosa diviene res signata, è ciò che si chiama documentazione."*

[138] Rileva C.M. BIANCA, *I contratti digitali*, in Studium iuris, 1999, pag. 1036 "E' stato detto che il documento informatico ha la caratteristica di essere indipendente dal supporto materiale. Ciò non è del tutto esatto, in quanto gli impulsi elettronici sono pur sempre una realtà materiale. Piuttosto va rilevato che, diversamente dal tipico documento giuridico, il documento informatico non ha un supporto cartaceo, pur prestandosi ad essere riprodotto su carta comune". Si può concordare con l'affermazione della materialità del documento elettronico, in quanto comunque residente su un supporto informatico, qualunque esso sia. Il pregio dell'affermazione criticata dall'A. sta però nel mettere in rilievo la piena fungibilità dell'elemento materiale nel documento informatico, al contrario del documento cartaceo. In altre parole, il documento informatico non perderà la sua natura per essere stato trasferito (o duplicato) da

invece che la diversità ontologica del documento informatico incida sulle sue potenzialità comunicative, e quindi sulle applicazioni e su alcuni importanti fenomeni giuridicamente rilevanti.

La nozione tradizionale di documento comprende un'ampia casistica, che si ripropone identica, dal punto di vista del valore giuridico, all'interno della categoria del documento informatico: nell'ambito dei documenti aventi rilevanza giuridica, ve ne sono infatti alcuni con efficacia privilegiata, dal punto di vista sostanziale e/o dal punto di vista probatorio[139]. E' il caso, nel diritto nazionale italiano, dei documenti provenienti dalle Pubbliche Amministrazioni [140] (inclusi i provvedimenti giurisdizionali), ed è anche il caso dell'atto notarile, pubblico[141] o autenticato[142], stante l'efficacia probatoria qualificata riconosciuta allo stesso e l'idoneità pressoché esclusiva a costituire titolo per la trascrizione o iscrizione nei registri della pubblicità immobiliare e commerciale di atti a contenuto negoziale o in genere interprivatistico. Tali documenti si caratterizzano:

---

un supporto all'altro, per esempio dallo hard disk di un computer ad un floppy, o ad un CD, né tanto meno, almeno allo stato attuale della tecnologia, potrà parlarsi di originali o di copie, su cui infra cap.VI

[139] E' appena il caso di precisare che la qualificazione formale del documento informatico, ai fini della rispondenza del documento ai requisiti di forma richiesti dall'ordinamento giuridico a fini di validità o probatori, è problema che si suppone risolto in senso positivo ai fini del presente lavoro. Sui requisiti formali del documento informatico cfr. tra gli altri cfr. G. FINOCCHIARO, *Firma digitale e firma elettroniche*, cit. passim.,U. BECHINI – M. MICCOLI, cit. passim, e E. SANTANGELO – M. NASTRI, *Firme elettroniche*, cit. pag. 1134..

[140] Sull'atto pubblico amministrativo informatico, che appare compreso nella dizione letterale dell'art. 15, secondo comma della legge 15 marzo 1997 n. 59, A. MASUCCI, in Enc. Dir., voce *Atto amministrativo informatico.*

[141] Nel vigore del D.P.R. 513/97, non contenente una apposita norma, si era dibattuto sulla possibilità di considerare ammesso dall'ordinamento, sulla sola base della disposizione generale dell'art. 15, secondo comma, della legge 59/97, l'atto pubblico informatico. Una serie di dati normativi, tra cui il D.Lgs. 39/93, facevano propendere per la soluzione positiva accolta da M. MICCOLI, *Documento e commercio telematico*, Milano, 1998, pag. 104 ss.; G. PETRELLI, *Documento informatico, contratto in forma elettronica e atto notarile*, in Notariato, 1997, pag. 583 ss.; M. C. ANDRINI, *Dal tabellione al sigillo elettronico*, in Vita Not., 1998, pag. 1788 ss.; l'espressa previsione nel D.P.R. 513/97 della sola autenticazione delle sottoscrizioni, e la totale mancanza di ogni indicazione relativa all'atto pubblico, giustificata in base ad un indirizzo di politica legislativa, indicavano la soluzione negativa (in tal senso R. ZAGAMI, cit. pag. 196 ss.; P. PICCOLI-G. ZANOLINI, *Il documento elettronico e la firma digitale*, in I problemi giuridici di Internet, a cura di E. Tosi,, Milano, 1999, pag. 97). L'articolo 9 del D.P.R. 445/2000, nel ribadire la possibilità dell'atto amministrativo informatico, usa espressioni di carattere più generale che sembrano far propendere per l'ammissibilità dell'atto notarile pubblico. L'articolo 13 del medesimo provvedimento, inoltre, prevede che libri scritture e repertori, ivi compresi quelli previsti dall'ordinamento del notariato e degli archivi notarili possono essere formati con strumenti informatici. Ciò rende chiara la tendenza del legislatore: tuttavia non sono state emanate le disposizioni attuative previste in tale norma. In realtà si deve rilevare che la questione risulta priva di attualità, in quanto la normativa presenta, in relazione all'atto notarile pubblico, carenze che non possono essere risolte sul piano interpretativo e che rendono impossibile l'attuazione dell'atto notarile informatico. In particolare non è prevista una modalità di conservazione del documento notarile pubblico, che sia conforme o compatibile con le modalità previste dall'ordinamento del notariato e degli archivi notarili per gli atti cartacei, e che si coordini con le stesse nell'ipotesi certa che i notai continuino a rogare atti notarili in forma cartacea, oltre a quelli in forma informatica. Sul punto infra diffusamente cap.VII.

[142] Espressamente ammessa e regolata dall'art. 24 del D.P.R. 445/2000. Sul punto M.MICCOLI, *Art. 16 Firma digitale autenticata*, in Le Nuove leggi civili commentate, I commentari, *Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, III-IV 2000, pag. 811, R. ZAGAMI, cit., pag. 184, E. SANTANGELO – M. NASTRI, cit. pag. 1149.

dal punto di vista formale-contenutistico per avere caratteristiche almeno in parte predeterminate (es. requisiti formali e di contenuto di sentenze, atti notarili, atti pubblici amministrativi, certificazioni[143]);

dal punto di vista della paternità per essere formati da un soggetto qualificato appartenente ad una Pubblica Amministrazione o munito comunque di un potere delegato dallo Stato.

La verifica dell'autenticità del documento e della sussistenza del potere in capo al suo autore necessita dell'ausilio del soggetto o dell'autorità da cui il potere deriva.

Nel caso di un atto amministrativo lo stesso conterrà gli elementi necessari per identificarne l'autore ed il suo ruolo. Nel caso della rappresentanza in materia civile e commerciale il documento conterrà l'enunciazione del conferimento dei poteri, da giustificarsi (in taluni casi obbligatoriamente mediante esibizione o allegazione del relativo atto) secondo le regole generali (nell'ordinamento italiano l'art. 1393 c.c. espressione di un principio generale [144], comune ai paesi di *civil law).*

In prima istanza pare quindi che l'intera questione della sussistenza dei poteri in capo ad un soggetto sia estranea ed ulteriore rispetto al meccanismo di firma. La verifica dell'autenticità di un documento cartaceo e della sussistenza in capo al soggetto che ne è autore dei poteri necessari a rendere impegnativo il documento per tutti i suoi destinatari può quindi essere effettuata ripercorrendo e controllando, fino al soggetto conferente, il percorso di conferimento dei poteri, e la permanenza degli stessi.

Tuttavia nel mondo del documento cartaceo i documenti, e quindi la loro provenienza e paternità, sono riconoscibili anche per un insieme di caratteristiche esteriori, quali la carta intestata, la protocollazione, le modalità di redazione e datazione e, non da ultimo, l'apposizione di timbri, sigilli, punzoni che caratterizzano e qualificano il documento e presentano alcune sommarie caratteristiche di sicurezza, sufficienti a garantire un'accettabile tutela dei traffici giuridici. Tale sistema empirico si giustifica con ragioni storiche e culturali, ma anche con l'estrema onerosità di un controllo generalizzato. Inoltre il trattamento del documento cartaceo è basato normalmente su contatti diretti e personali tra i soggetti interessati (presentazione e ritiro agli sportelli, richieste di chiarimenti, contatti tra pubbliche amministrazioni) che costituiscono mezzi impliciti di controllo dell'autenticità.

Nessuna di queste caratteristiche è presente nel documento informatico. Esso esclude per sua natura ogni contatto diretto tra autore e destinatari e non è suscettibile dell'apposizione di segni esteriori quali, ad esempio sigilli, timbri, punzoni[145]. Pertanto la normativa italiana di settore espressamente prevede che l'apposizione della firma digitale (ed ora elettronica) integra e sostituisce l'uso di tali mezzi[146]. Ciò però rende

---

[143] Sull'atto notarile pubblico G. CASU, *L'atto notarile tra forma e sostanza*, Milano-Roma, 1996, pag. 7ss.; G.MARICONDA, *Atto Pubblico*, in Enc. Giur. Roma, 1989, pag. 1. Sull'atto pubblico in genere G. CRISCI, *Atto Pubblico (diritto civile)* in Enc. Dir, IV Milano, 1959, pag. 265 ss.; sulla certificazione A.STOPPANI, *Certificazione*, in Enc. Dir., VI,Milano, 1960, pag. 793, e specificamente sulla graduazione dell'efficacia probatoria per i vari tipi di certificazione pag. 794.

[144] F. SANTORO-PASSARELLI, *Dottrine*, cit. pag. 282, R. SCOGNAMIGLIO, *Contratti in generale*, 3^ ed., 2^ rist. Milano, 1977 pag. 69; G. MIRABELLI, *Dei Contratti in generale*, 3^ ed. Torino, 1980, pag. 376.

[145] O meglio tali segni esteriori non forniscono alcuna garanzia in quanto facilmente riproducibili da chiunque.

[146] art. 24 comma 3, art. 25, comma 2, D.P.R. 445/2000. Per un collegamento tra tali norme e le modalità di rilascio delle firme digitali dei pubblici ufficiali cfr. G.FINOCCHIARO *La Firma digitale*, cit. pag. 208.

necessario, al momento dell'utilizzazione, il controllo, quanto meno nel settore pubblico, della provenienza del documento da soggetto abilitato alla sua emissione, con la conseguente necessità di inserire all'interno del processo della firma digitale[147] l'indicazione di funzioni, qualifiche, poteri, cariche. Gli usi cui taluni documenti sono destinati rendono perciò necessario che la provenienza ed autenticità siano garantiti al terzo destinatario od utilizzatore, e quindi all'intera collettività (validità *erga omnes*).

Una simile osservazione è corollario della premessa da cui siamo partiti: la non assimilabilità dal punto di vista ontologico, ma solo dal punto di vista contenutistico e degli effetti, del documento informatico al documento cartaceo. La differenza sul piano fenomenico, culturale e sociologico non può non divenire, almeno in parte, differenza sul piano del trattamento giuridico.

Ma vi è di più: l'intero percorso evolutivo del documento informatico rende evidente un particolare fenomeno, che solo la consistenza e la velocità del cambiamento in atto hanno reso possibile; la gestione del documento cartaceo è basata su tecniche e sistemi socialmente accettati e diffusi fino al punto di essere considerati solo implicitamente nella normativa, mentre la gestione del documento informatico necessita di una preventiva esplicitazione analitica di tutti i processi. La locuzione firma digitale, come è stato sin dall'inizio notato ed è ricordato anche nel corso di questo lavoro, contiene un'implicita imprecisione consistente nell'assimilazione di fenomeni dissimili, che è già stata causa di equivoci ed errori.

Per tutte queste ragioni è necessaria, per il documento informatico, una modalità di verifica della sussistenza in capo al soggetto firmatario di funzioni, qualifiche o poteri, che sostituisca le modalità empiriche di prima verifica del documento tradizionale, e si adegui alle potenzialità proprie del documento informatico, come ad esempio il trattamento con procedure automatiche.

D'altro canto occorre anche chiedersi se il nuovo strumento tecnologico possa offrire modalità operative che possano garantire un più facile accertamento della sussistenza di poteri in capo ai singoli soggetti.

Occorre quindi considerare le potenzialità del meccanismo della firma digitale, per comprendere quali siano i possibili metodi per l'accertamento di un potere in capo ad un soggetto.

Il collegamento della coppia di chiavi di firma (pubblica e privata) al soggetto che ne è titolare è fatta[148], sotto la responsabilità del Certificatore quale terza parte fidata, attraverso il certificato di firma: questo a sua volta non è altro che un documento informatico, redatto secondo standard internazionali recepiti dalla normativa nazionale[149], nel quale sono contenuti i dati che consentono di attribuire ad un soggetto

[147] In linea puramente teorica si può ipotizzare un percorso di controllo manuale, risalendo la catena autorizzatoria che porta ai poteri dell'autore del documento. Tuttavia immaginare di risalire, specialmente nel caso di una pubbica amministrazione, ai poteri del soggetto autore del documento, lungo la catena gerarchica attraverso un percorso omogeneo di verifica, è incompatibile con le normali esigenze operative. Occorre quindi un meccanismo che consenta una verifica *a priori*, attualmente disponibile, come vedremo, solo nell'ambito dei sistemi di firma elettronica basati sulla certificazione delle chiavi asimmetriche.

[148] Una dettagliata descrizione del procedimento in M.MICCOLI, *Documento e commercio telematico*, Milano, 1998, pagg. 2 ss.

[149] La norma dell'art. 12 del D.P.C.M. 8 febbraio 1999 prescriveva precisi requisiti tecnici. A seguito della revisione della normativa di cui al D.P.C.M. 13 gennaio 2004, è scomparso ogni riferimento a standard tecnici, e permangono prescrizioni relative a contenuto del certificato, modalità di rilascio, funzionalità e sicurezza, in aderenza a quanto prescritto dalla Direttiva 99/93/UE, volta a favorire il mercato in materia di firme elettroniche, e quindi a non vincolare le scelte tecnologiche.

la titolarità della coppia di chiavi. In tale documento è astrattamente possibile (ed è previsto dagli standard tecnici) l'inserimento di una particolare qualità del soggetto titolare, quale ad esempio un ruolo od un potere di rappresentanza.

In ragione di ciò la possibilità di indicare poteri, funzioni, o più genericamente, attributi del titolare, è legislativamente prevista all'art. 6, commi 3 e 4 della Direttiva 1999/93/CE, ed all'articolo 28 bis del D.P.R. 445/2000, come novellato dall'articolo 7 del D.Lgs. 10/2002. In molti casi poi, in cui l'enunciazione di funzioni non costituisce un'esigenza irrinunciabile, essa appare utile per fornire adeguati livelli di sicurezza e per attivare procedure automatiche di verifica, che rendano, in ultima analisi, il sistema affidabile e conveniente agli occhi dell'utenza.

La normativa di settore mostra di avvertire il problema, ma detta solo criteri generali per la soluzione. Ciò si spiega con la novità del mezzo, con la mancanza di esperienze applicative, e con la scelta, prima del legislatore comunitario e poi anche di quello nazionale, di non intervenire normativamente nelle caratteristiche tecniche della firma elettronica. Non vi sono infatti norme specifiche in materia di rappresentanza volontaria od organica, e si devono ritenere applicabili i principi generali, e vi sono solo scarne indicazioni in materia di pubbliche amministrazioni e pubbliche funzioni.

Esaminiamo brevemente i principali dati normativi.

La Direttiva 99/93/CE definisce firmatario "… persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta[150]" (art.2, comma 3); nell'allegato 1, relativo ai requisiti prescritti per un certificato qualificato, è prevista all'interno di tale tipo di certificato l'indicazione di un attributo specifico del firmatario.

L'art. 27 bis del D.P.R. 445/2000 dispone tra l'altro:

3. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

L'art. 29 bis del D.P.R. 445/2000 statuisce[151]:

---

[150] E' discutibile se il certificato di firma possa essere rilasciato a soggetto diverso da una persona fisica. Il DPR 513/97, ed il D.P.R. 445/2000, nelle formulazioni originarie, non contenevano indicazioni specifiche, utilizzando espressioni ambivalenti, fatta eccezione per il comma 4 dell'art. 29. Una serie di indicazioni in senso positivo, in verità poco coordinate e talvolta contraddittorie, derivavano dal D.P.C.M. 8 febbraio 1999 ed in particolare dagli articoli 11 e 62, e sono fortunatamente scomparse nel D.P.C.M. 13/1/2004. La Direttiva europea 99/93/CE appare andare nella direzione di escludere la possibilità del rilascio di un certificato ad una persona giuridica o ad un ente privo della personalità giuridica. La dizione dell'art. 2 sembra riferirsi in modo inequivocabile alla persona fisica; così anche il riferimento al "nome" del firmatario contenuta nell'allegato I. Infine gli standard tecnici internazionali non sembrano allo stato comprendere la possibilità dell'attribuzione del certificato di firma a soggetto diverso da una persona fisica. Anteriormente all'emanazione della Direttiva, nel senso dell'ammissibilità di un certificato rilasciato a soggetto diverso da persona fisica L. GATT, C*ommento agli artt. 8 e 9 del D.P.R. 513/97*, in Le Nuove leggi civili commentate, I commentari, Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici, III-IV 2000, pag. 710. Contra G. FINOCCHIARO, *Documento informatico e firma digitale*, in Contratto e Impresa, 1998, pag. 987.

[151] Tale norma sostituisce l'art. 28, comma 2, del D.P.R. 445/2000 (già art.9, comma 2, D.P.R. 513/97), che, nella versione previgente, tra gli obblighi del certificatore imponeva di "identificare con certezza la persona che fa richiesta della certificazione", di "specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza di poteri di rappresentanza o di altri titoli relativi all'attività

Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati è tenuto inoltre a:

omissis

c) specificare, nel certificato qualificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi;

omissis

h) procedere alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;

L'art. 29 septies del D.P.R: 445/2000 recita:

1. Il certificato qualificato deve essere a cura del certificatore:

omissis

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente decreto;

L'art. 29 quinquies del D.P.R. 445/2000, introdotto del D.P.R. 7 aprile 2003 n. 137 sancisce[152]:

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tal fine l'obbligo di accreditarsi ai sensi dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei ministri, su proposta dei Ministri della funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

omissis

---

professionale o a cariche rivestite" e di "procedere tempestivamente alla revoca o sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo".

[152] Tale norma sostituisce e modifica il previgente art. 29 che così recitava:

Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza

Con il decreto di cui all'articolo 8 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni

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'ambito dei rispettivi ordinamenti giuridici.

Le chiavi pubbliche di ordini ed albi professionali legalmente riconosciuti e dei loro legali rappresentanti sono certificate e pubblicate a cura del Ministro di grazia e giustizia o suoi delegati.

3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.

4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche di cui all'articolo 8, comma 2.

Infine, solo per inciso, va detto che anche la normativa italiana sul processo telematico, tuttora in attesa di piena attuazione, prevede per l'accesso una modalità di verifica delle funzioni e delle abilitazioni[153].

Il quadro che risulta da tale contesto normativo, da coordinare con l'ordinamento giuridico generale, è sempre più, anche alla luce delle recenti modifiche, quello di una cornice da definire sulla base della pratica e delle normative attinenti il singolo campo applicativo. La derivazione diretta di alcune norme dalla Direttiva Europea (generale per definizione in quanto sovrapponibile a differenti ordinamenti giuridici) rafforza questo inquadramento.

Per l'applicazione di tale normativa al notariato occorre quindi distinguere il senso delle varie norme in relazione agli istituti di diritto nazionale cui vanno applicate.

Per quanto attiene la rappresentanza di diritto privato, risulta chiara la possibilità che la *contemplatio domini* sia effettuata all'interno del meccanismo della firma digitale. Ciò è esplicitato nel combinato disposto delle norme di cui ai novellati articoli 27 bis, 29 bis e 29 septies del D.P.R. 445/2000, che delineano un quadro in cui l'enunciazione del potere rappresentativo viene effettuata con il consenso, e sotto la responsabilità, di tre distinti soggetti: il Certificatore, che indica la funzione nel certificato di firma, il titolare della firma, che ne richiede l'inserimento (e può essere limitato all'uso di tale firma digitale solo nei casi di esercizio della specifica funzione), ed il soggetto da cui promana il potere (alternativamente "*terzo*" o "*terzo interessato"* nella normativa di settore[154]).

Ciò rileva nella fase di rilascio del certificato di firma, ma anche in quelle della sospensione e della revoca della firma stessa, che dipendono tutte non solo da situazioni e circostanze relative al titolare, ma anche dalle vicende dei suoi poteri. Simmetricamente, vi sarà responsabilità del Certificatore, o del titolare, o del terzo

[153] Il D.P.R. 23 febbraio 2001 n. 123 stabilisce all'art. 3 che le norme per l'accesso dei difensori delle parti e degli ufficiali giudiziari al sistema informatico civile sono stabilite con Decreto del Ministro della Giustizia, sentita l'Autorità per l'Informatica della Pubblica Amministrazione. Tale Decreto, al momento in cui si scrive, non è stato ancora emanato.

[154] Tale genericissima locuzione è espressione del tentativo di definire unitariamente situazioni non rientranti in un'unica categoria dogmatica tradizionale. Non può condividersi, pertanto, l'opinione che identifica nel rappresentante il *terzo interessato, (*P. TROIANO, C*ommento all'art. 9, lett. C) del D.P.R. 513/97*, in Le Nuove leggi civili commentate, I commentari, cit., pag. 725 ss.) in quanto in primo luogo la stessa non giustifica in alcun modo una diversa definizione normativa per un soggetto che, in fin dei conti, è pur sempre il titolare, ed in secondo luogo non tiene conto della funzione della norma, che vale a definire obblighi e responsabilità del Certificatore all'atto dell'indicazione nel certificato di firma della sussistenza di poteri. Nel senso del testo L. ALBERTINI, *Sul documento informatico e sulla firma digitale*, in Giust. Civ., 1998, II, pag. 285.

interessato, qualora un certificato sia rilasciato, o rimanga attivo, quando il suo contenuto non corrisponda alla realtà, e si ingeneri un erroneo affidamento nei terzi[155].

Analogo schema va adottato per la certificazione della sussistenza di una abilitazione professionale[156] In tal caso occorre riferirsi, oltre che alle norme già citate, anche alla norma contenuta nell'articolo 29 quinquies del D.P.R. 445/2000, introdotta di recente senza alcun coordinamento con le norme previgenti. Tale norma prevede l'introduzione di regole specifiche per le professioni, sulla base dei principi generali previsti dai rispettivi ordinamenti, in virtù di Decreto del Ministro per l'innovazione e le tecnologie. Nelle more dell'emanazione di tale Decreto, si applicano le regole del Decreto di cui all'art. 8, comma 2, del D.P.R. 445/2000.[157] Allo stato si deve ritenere che l'unica modalità per accertare la sussistenza di un'abilitazione professionale nel rispetto della normativa di settore e dei principi generali dei rispettivi ordinamenti, sia quello di riferire la certificazione della sussistenza dell'abilitazione al soggetto deputato alla tenuta dell'Albo professionale, e quindi al locale ordine professionale (stante la abituale ripartizione su base territoriale di tali organismi) e per esso al suo presidente.

In tale quadro assumeva una specifica funzione la previgente norma dell'ultimo comma dell'articolo 29 del D.P.R. 445/2000 (nella sua formulazione originaria) che prevedeva il rilascio da parte del Ministro della Giustizia delle chiavi di firma dei legali rappresentanti degli Ordini Professionali. In tal modo può essere garantita, nell'ambito di una struttura gerarchica, l'effettività della certificazione, da parte dei Presidenti, dell'appartenenza di un soggetto ad un Ordine e dell'attualità di tale appartenenza.[158]. La normativa attuale, in attesa dell'emanazione del previsto Decreto del Ministro per l'Innovazione e le Tecnologie, consente tale soluzione, peraltro in corso di attuazione pratica[159], pur senza più considerarla vincolante. Va tuttavia precisato che, anche dopo la modifica normativa, il richiamo ai principi generali rende obbligata un'impostazione del sistema del tipo di quella prospettata.

Più complessa è la strutturazione del sistema delle pubbliche amministrazioni. La normativa distingue tra usi interni ed usi esterni della firma digitale, per i quali occorre in ogni caso che le firme siano rilasciate da un Certificatore accreditato. Questo può essere la stessa Pubblica Amministrazione[160], che deve tuttavia preventivamente

---

[155] Afferma un principio di responsabilità per tutti gli utenti della firma digitale, ammettendo la ripartizione delle stesse per categorie di utenti L.GATT, *Commento agli artt. 8 e 9 del D.P.R. 513/97*, in Le Nuove leggi civili commentate, cit. pag. 710. L'A. conclude per "un ampio potere di valutazione da parte del giudice delle circostanze concrete, dovendo tale valutazione avere riguardo: 1) alla categoria (o alle categorie) di soggetto telematico cui l'utente appartiene; 2) al tipo di attività di utilizzazione posta in essere; 3) alla comparazione tra comportamento tenuto e comportamento che l'utente avrebbe dovuto tenere in relazione ai due parametri suddetti".

[156] Ci si riferisce alle cd. professioni protette, non rilevando l'enunciazione nel certificato di firma digitale dell'esercizio di attività non subordinate ad una abilitazione.

[157] Allo stato si tratta del D.P.C.M. 13 gennaio 2004 che, come il precedente D.P.C.M. 8 febbraio 1999, che non contiene alcuna prescrizione al riguardo.

[158] Sulle problematiche sollevate dall'ultimo comma dell'articolo 17 del D.P.R. 513/97, poi integralmente trasfuso nell'art. 29 del D.P.R. 445/2000, e sulla sostanziale equivocità del testo, cfr. F. COCCO, *Art. 17, Chiavi di cifratura della Pubblica Amministrazione*, in Le Nuove leggi civili cit. pag. 816-817.

[159] Il Ministero della Giustizia italiano ha infatto rilasciato, nel corso del 2003, le firme digitali al Presidente del Consiglio Nazionale del Notariato ed a tutti i consiglieri nazionali, ed è in corso di attivazione la procedura per il rilascio delle firme digitali ai Presidenti dei Consigli Notarili Distrettuali, da utilizzarsi per tutte le comunicazioni ufficiali ed in particolare per le comunicazioni con gli organi locali e centrali del Ministero della Giustizia e dell'amministrazione giudiziaria.

[160] E' il caso dell'Esercito Italiano, che si è iscritto all'albo dei certificatori nel corso del 2003.

sottoporsi alle procedure di accreditamento, od un Certificatore accreditato che rilasci certificati di firma alla Pubblica Amministrazione, per gli usi con rilevanza esterna[161]. In tale ambito dovranno essere strutturati i sistemi per la certificazione delle funzioni.

Resta da esaminare il trattamento che la normativa riserva ai pubblici ufficiali ed in particolare, tra questi, ai notai. Anche qui l'impianto normativo è stato di recente modificato[162], e si rinviene il permanere di un diverso trattamento rispetto sia alle attività professionali, sia alle pubbliche amministrazioni.

Le modalità di indicazione di una qualifica professionale risultano infatti sia dalle norme dei novellati articoli 27 bis, 29 bis e 29 septies del D.P.R. 445/2000, sia dalla norma dell'art. 29 quinquies, anch'essa di nuova introduzione.

I pubblici ufficiali sono invece presi in considerazione solo da quest'ultima norma, che riproduce, con modifiche, il previgente articolo 29. Se non si vuole ricondurre il tutto ad un errore compilativo, occorre ritenere che permanga un intento del legislatore di disciplinare diversamente le firme digitali dei pubblici ufficiali, rispetto a quelle dei liberi professionisti, anche nei casi in cui, come per il notaio, la qualifica di pubblico ufficiale si cumuli a quella di libero professionista. E' da ritenere, infatti, che prevalga, nel trattamento del documento informatico, la funzione pubblicistica del notaio, rispetto a quella libero professionale.

D'altra, parte dall'impianto normativo risulta per i notai, più ancora che in precedenza, un semplice rinvio all'ordinamento di settore. In attesa dell'emanazione del previsto decreto, che potrà in qualche punto discostarsi dalle specifiche norme dell'ordinamento del notariato, in ragione della peculiarità del fenomeno regolato, mantenendo tuttavia salva la fedeltà ai principi generali[163], occorre quindi far riferimento all'intero *corpus* dell'ordinamento notarile.

Tra i principi generali che non potranno essere ignorati, in sede di emanazione del previsto decreto ministeriale, sono essenziali il potere di autonomia amministrativa spettante all'ente collegio notarile in relazione ai propri iscritti[164], di cui è corollario il potere di vigilanza e controllo dei Consigli Notarili Distrettuali, il tutto a tutela della funzione pubblica e conseguentemente della collettività.

E' naturale che la verifica della funzione notarile sia effettuata là dove è tenuto il Ruolo dei notai[165], e quindi presso i Consigli. Ciò non significa solo l'esercizio di un potere-dovere di certificazione, ma la rispondenza di tale prerogativa ad un più ampio compito di controllo, vigilanza e tutela.

---

[161] Una disamina delle varie possibili modalità di certificazione delle firme nella P.A. in G. FINOCCHIARO, La firma digitale, cit. pag. 201 ss., ed in F.COCCO, op. cit., pag. 817.

[162] Scompare per i notai in quanto ordine, l'obbligo di rilascio delle firme digitali ai legali rappresentanti, su cui *supra* nel testo. Già critico verso questa norma, di oscuro senso, F. COCCO, cit. pag. 818.

[163] Secondo G. FINOCCHIARO, *La firma digitale*, cit, pag. 208, che commenta la norma dell'art. 17 del D.P.R. 513/1997, "Il rinvio è quindi da intendersi all'autonomia normativa degli ordini, ove sia ad essa riconducibile, o delle categorie di appartenenza e alla eventuale specifica disciplina sulla firma, da intendersi comprensiva della regolamentazione dell'uso di sigilli, timbri e punzoni che, come sancisce l'art. 18, la firma digitale sostituisce." Tali considerazioni sembrano tuttora valide in relazione al novellato dettato normativo.

[164] C. FALZONE A. ALIBRANDI, Dizionario Enciclopedico del Notariato, I, voce Collegi Notarili, pag. 547.

[165] Il rilievo sostanziale del Ruolo notarile si rileva dalla disciplina degli effetti. Infatti una volta iscritto a ruolo il notaio può esercitare le sue funzioni. Eventuali atti rogati precedentemente sarebbero nulli ex art. 58 l.n.. Cfr. P. BOERO, *La Legge Notarile Commentata*, Torino, 1993, pag. 148.

Il Ruolo dei Notai contiene infatti tutti i dati rilevanti per l'esercizio della pubblica funzione da parte del notaio, e quindi le generalità, la data dell'esame di concorso, la data del decreto di nomina o di trasferimento, la residenza del notaio e la cauzione prestata, le pene ed i provvedimenti disciplinari, la riabilitazione avvenuta.

Risulta quindi evidente l'interesse pubblico alla regolare tenuta del Ruolo dei notai[166], e la necessità di tener conto di tale disciplina anche nell'applicazione della normativa in materia di documenti informatici e firme elettroniche.

Il rilascio delle firme elettroniche dei notai è pertanto soggetto alle stesse regole che abilitano il notaio all'esercizio della professione secondo l'ordinamento professionale: così come il Presidente del Consiglio Notarile Distrettuale[167], ai sensi dell'art. 24 della legge 16 febbraio 1913 n. 89, ordina l'iscrizione nel Ruolo dei notai esercenti nel Distretto, e da tale momento il notaio è abilitato all'esercizio, sarà il Presidente del Consiglio Notarile a procedere al rilascio (o ad intervenire necessariamente nella fase di rilascio) della firma digitale relativa all'esercizio delle funzioni notarili[168]. Analogamente le procedure di sospensione e revoca della firma devono essere modulate sulle procedure relative alla interruzione o alla cessazione dall'esercizio delle funzioni notarili, e tali cause di sospensione e revoca si aggiungeranno a quelle proprie di qualunque firma elettronica[169].

L'enunciazione, all'interno del meccanismo di firma digitale, ed in modo conforme alla normativa, della sussistenza di funzioni, poteri, qualifiche consente quindi di risolvere in modo preventivo alcune questioni fondamentali circa l'imputabilità del documento informatico e la sua efficacia sostanziale e probatoria.

Il soddisfacimento dei vincoli posti dalle norme esaminate non comporta tuttavia l'applicazione di procedure o tecnologie normativamente predeterminati[170]. La normativa lascia piena libertà circa le modalità di indicazione delle funzioni.

---

[166] C. FALZONE A. ALIBRANDI, op. cit., III, pag. 573, così esplicita le funzioni del Ruolo: "L'iscrizione a ruolo serve a garantire all'esterno che il notaio ha osservato le minuziose regole poste a garanzia dei terzi e determina il duplice effetto di inserire il notaio nel collegio, come membro, assoggettandolo alla particolare vigilanza di quest'ente, e di consentirgli di instaurare contratti d'opera professionale con i privati. Trattasi di due effetti tra loro influenti reciprocamente, in quanto la possibilità di instaurare rapporti professionali è concessa nel momento in cui l'ente professionale collegio può vigilare sulla condotta del notaio ed eventualmente reagire nei dovuti modi a violazione di norme; d'altro canto ha senso l'inserimento del notaio nel collegio, se il professionista è abilitato a svolgere le sue funzioni. La nullità dell'atto rogato prima dell'iscrizione costituisce un espediente sanzionatorio, in primo luogo per indurre il notaio a non prestare la propria opera prima dell'iscrizione, secondariamente per garantire i privati che l'opera professionale è esplicata entro i limiti previsti dalla legge".

[167] Il presidente del Consiglio Notarile Distrettuale è munito della funzione generale della rappresentanza dell'ente ai sensi dell'art. 97 Reg. Not. (R.D. 10 settembre 1914 n. 1326), ed è "caratterizzato da una duplice funzione, una avente stretta attinenza con l'attività del consiglio, ed una che prescinde assolutamente da riflessi sulla azione del consiglio", C. FALZONE A.ALIBRANDI, op.loc. cit. Conforme P. BOERO, op.cit., pag. 545;

[168] In tal senso, sia pure nell'ambito di un più ampio ventaglio di ipotesi M. MICCOLI, *Documento e commercio telematico*, cit. pag. 115.

[169] Commissione Informatica del Consiglio Nazionale del Notariato, Proposta per la realizzazione di una infrastruttura a chiave pubblica per la Pubblica Amministrazione, in CNN-NOTIZIE 4 agosto 1999, n. 150.

[170] La normativa nazionale, ed in particolare il D.P.C.M. 8 febbraio, contenevano (ed ancora contengono in regime transitorio anche nel vigore dell'attuale D.P.C.M. 13 gennaio 2004), riferimenti a norme tecniche. Tali riferimenti tendono a scomparire in ottemperanza ai principi della Direttiva. Tuttavia la problematica in esame non è mai stata oggetto di autonoma regolamentazione, anche dal punto di vista tecnico.

Ciò ha comportato non pochi problemi, in assenza di standard tecnici internazionalmente riconosciuti.

Allo stato infatti non esistono standard internazionalmente riconosciuti che consentano la diretta verifica, all'interno del complessivo sistema della firma digitale, di funzioni, poteri, abilitazioni professionali di un soggetto[171]. Il Consiglio Nazionale del Notariato ha realizzato un sistema che consente di garantire l'accertamento preventivo delle funzioni in capo al titolare della firma digitale, utilizzato attualmente anche dal Consiglio Nazionale Forense per gli avvocati, ed ha contribuito alla realizzazione di un sistema applicabile anche ad ipotesi prive della peculiare semplicità propria degli Ordini Professionali.

La difficoltà nell'avvio di tali applicazioni, che solo ora sembra in via di superamento, è da imputarsi a motivi tecnici e giuridici. Dal punto di vista giuridico, l'estrema sinteticità delle norme non favorisce scelte univoche che garantiscano soluzioni con validità generale. Dal punto di vista tecnico, è possibile teoricamente agire in vari modi per l'attribuzione di funzioni o poteri, che possono essere così sintetizzati, con le rispettive caratteristiche ed inconvenienti:

- l'indicazione di poteri o funzioni direttamente nel Manuale Operativo[172], collegando così ad un Certificatore esclusivamente soggetti aventi una determinata funzione (es.: le firme digitali del Certificatore Consiglio Nazionale del Notariato, sono rilasciate esclusivamente a notai in esercizio, e ciò risulta dal Manuale Operativo, in tale scia si è posta l'Autorità di Certificazione del Consiglio Nazionale Forense, per gli avvocati); tale soluzione aggira le problematiche di carattere tecnico, ma, a causa dell'unicità del Manuale Operativo per ogni Certificatore, può adottarsi esclusivamente nei casi in cui la qualifica da attribuire sia unica, come per il Notariato e le altre professioni; non è quindi applicabile a tutte le strutture gerarchiche, come nel caso della Pubblica Amministrazione, e costituisce soluzione ad una limitata classe di problemi;[173]

- l'inserimento nel certificato di firma digitale di un campo cd. di estensione che indichi i poteri; tale soluzione, presente nella normativa nazionale[174], e compatibile con quella comunitaria, appare la più facilmente realizzabile in un futuro prossimo, ma necessita di un processo di standardizzazione delle procedure tecniche ed organizzative, perché le indicazioni dei poteri risultino con certezza all'atto dell'utilizzazione e della verifica della firma, come richiesto dalle norme che determinano le responsabilità del Certificatore (art. 28 bis D.P.R. 445/2000)[175];

---

[171] Esistono nella pratica casi di indicazione delle funzioni all'interno del certificato di firma digitale, ma le modalità di tali indicazioni sono tali da non garantire con certezza che queste appaiano al terzo fruitore di un documento firmato; inoltre, nei manuali operativi dei Certificatori che inseriscono tali indicazioni, sono spesso presenti limitazioni di responsabilità volte a rendere le stesse non impegnative.

[172] Il Manuale Operativo è la traslazione nell'ordinamento nazionale delle *CPS (Certificate Practice Statements)* e della *policy* quali definite dalla letteratura tecnica internazionale. Esso è previsto dal D.P.C.M. 13 gennaio 2004 all'articolo 38. Fermo restando che il manuale operativo non può intervenire su quanto regolato da norme inderogabili, si ritiene che la sua funzione sia appunto quella di specificare le modalità e finalità dell'esercizio dell'attività da parte del certificatore, i suoi rapporti con i terzi ed anche alcune limitazioni come quella prevista nel testo.

[173] essa è stata adottata dal Notariato in quanto unica scelta immediatamente praticabile.

[174] art. 29 bis, lett. C) del D.P.R. 445/2000, come novellato dal D.Lgs. 10/2002,,

[175] in tale prospettiva è stata l'attività del Gruppo di lavoro coordinato dal Consiglio Nazionale del Notariato nell'ambito dell'Assocertificatori (associazione di categoria cui aderiscono la maggioranza dei Certificatori italiani della firma digitale) che ha realizzato ed ultimato, nell'anno 2003, le linee guida di uno standard tecnico e giuridico-organizzativo ed è in corso di distribuzione da parte dei Certificatori Associati a soggetti appartenenti alle Pubbliche Amministrazioni e ad altri Ordini Professionali, che non

- il collegamento al certificato cd. di firma, che individua il titolare, di un secondo certificato cd. d'attributo[176], che ne individua le funzioni o, traducendo dall'inglese, le attribuzioni; anche questa modalità è teoricamente possibile, e presenta l'innegabile vantaggio di consentire una vita del certificato di firma distinta da quella del certificato di attributo, ed anche la certificazione dell'attributo da parte di Certificatore diverso dal Certificatore della firma[177]; tale modalità non è tuttavia espressamente prevista dalla normativa, e ciò comporta non pochi problemi di coordinamento; in linea di fatto poi, essa risulta ancora non praticabile per i ritardi nell'elaborazione di uno standard riconosciuto da tutte le applicazioni di firma digitale presenti sul mercato, con i conseguenti insormontabili problemi di interoperabilità. Allo stato sono in corso, in particolare a livello europeo, studi per la standardizzazione del certificato di attributo e per l'individuazione delle applicazioni per le quali utilizzarlo[178] .

La prima di queste ipotesi, che si fonda su in presupposto organizzativo e non tecnologico, è attualmente praticata, nel caso dell'autorità di certificazione del Consiglio Nazionale del Notariato ed in quella del Consiglio Nazionale Forense. L'indicazione delle funzioni nelle cd. estensioni del certificato, praticabile e già in parte praticata, ma in attesa di regole o accordi tecnici che ne consentano una piena interoperabilità, costituisce un sistema utile in senso generale anche per le strutture gerarchiche, ed ha una prima diffusione, anche grazie al modello realizzato da Assocertificatori su impulso del Consiglio Nazionale del Notariato, nell'ambito di rapporti convenzionali tra Certificatori e Pubbliche Amministrazioni. Entrambi tali sistemi presentano l'inconveniente di limitare l'uso della firma al caso di esercizio del potere o della funzione ad essa legato, ed in essa contenuto.

Migliori prospettive offre il certificato di attributo; ma si tratta di tecnologia non ancora matura.

Tutte tali ipotesi avrebbero quindi potuto essere applicate al notariato[179]. I Presidenti dei Consigli Notarili Distrettuali intervengono infatti, sulla base dello schema normativo in precedenza esposto, nella fase di rilascio delle chiavi di firma dei notai, allo scopo di garantire la sussistenza della funzione notarile; successivamente controllano il ciclo di vita delle chiavi in relazione sempre alla sussistenza in capo al soggetto di tali funzioni. Ciò è realizzabile sia nell'ipotesi dell'autorità di certificazione

---

hanno realizzato la propria Autorità di Certificazione. Maggiori ragguagli su tale esperienza sono disponibili all'indirizzo http://www.assocertificatori.org.

[176] In effetti sarebbe teoricamente possibile una quarta possibilità, consistente nel collegamento ad un soggetto, per l'attribuzione di funzioni, di due distinte chiavi di firma, il cui uso contemporaneo consenta di ritenere verificata la sussistenza della funzione e la volontà di agire nell'esercizio della stessa. Tale ipotesi appare tuttavia incompatibile con la normativa vigente, che non regola ad esempio il caso dell'uso di una sola di tali chiavi, non equiparabile quindi alla firma. Il novero delle possibili soluzioni al problema potrebbe evidentemente ulteriormente allargarsi: ciò tuttavia non ha alcuna rilevanza in mancanza di uno specifico riconoscimento da parte dell'ordinamento giuridico.

[177] Prospettiva questa particolarmente interessante per il Consiglio Nazionale del Notariato, che avrebbe potuto assumere la funzione di Certificatore di attributo (o di funzione). Cfr. *Commissione Informatica del Consiglio Nazionale del Notariato*, cit.

[178] Un'ipotesi concreta di utilizzazione del certificato di attributo è sviluppata in *N.* MAZZOCCA, A. MAZZEO, M. NASTRI, F. ROLLERI, L. ROMANO,.E. SANTANGELO, *Architettura e protocolli di rete di un'infrastruttura a chiave pubblica per la Pubblica Amministrazione*, in *Riv. Di Informatica*, vol. XXIX, n. 2 maggio-agosto 1999, pagg. 149 ss.; un'applicazione di tale ipotesi al notariato in M. NASTRI, *La firma digitale*, in Noter-Notariato dell'Emilia Romagna, n. 7, gennaio-giugno 1999, pag. 9 ss.

[179] U.BECHINI, Vademecum minimo in tema di funzione notarile e firma digitale, in Riv.Not. 5/2000, pag. 1155 ss.

autonoma del notariato, sia nelle ipotesi di utilizzazione del sistema basato sulle estensioni del certificato di sottoscrizione o sul certificato di attributo[180].

In ciascuna di queste ipotesi è tutelato un sistema di enunciazione delle funzioni che evidenzia i soggetti interessati, ne impone la partecipazione attiva alla procedura, e ne predetermina il regime di responsabilità in modo adeguato al sistema tecnologico ed al *corpus* normativo della firma digitale.

La scelta del Notariato di porsi in autonomia come certificatore dei notai è stata basata sulla constatazione della inesistenza, al momento della decisione (presa in via definitiva nella primavera del 2001), di una soluzione alternativa che consenta, come richiesto dalla normativa, da una parte l'evidenza della funzione notarile all'atto dell'apposizione della firma, e dall'altra il controllo delle funzioni da parte dei Consigli Notarili per tutti i casi di cessazione o sospensione.

Ma vi è di più. Il panorama delle firme elettroniche, dopo la Direttiva 99/93/CE, ed il D.Lgs. 10/2002, si è ulteriormente articolato, per non dire complicato, in virtù delle nuove figure previste, quali la firma elettronica semplice distinta dalla firma elettronica avanzata, quest'ultima basata o meno su un certificato qualificato e creata eventualmente con un dispositivo sicuro per la creazione della firma, e rilasciata da un Certificatore che sia o meno accreditato. Senza voler entrare nel dedalo di ipotesi che ne derivano, va chiarito che la Direttiva ha ritenuto di dare cittadinanza e dignità di firma praticamente ad ogni sistema di imputazione ad un soggetto di un documento informatico, allo scopo di impedire che gli stati nazionali scoraggino normativamente l'utilizzo di firme elettroniche, e di soddisfare le diverse esigenze provenienti dai paesi membri. Ne è conseguenza però un generale alleggerimento[181] del sistema originariamente previsto dal legislatore italiano, che equiparava la firma digitale alla sottoscrizione manuale solo se conforme a precisi requisiti tecnici. Basti pensare che non sussiste ormai, per nessun certificatore di firma digitale, l'obbligo di iscrizione a pubblici elenchi, che resta una mera facoltà.

Questa situazione, unita al continuo susseguirsi di modifiche normative più o meno importanti (ma spesso molto importanti) comporta l'importanza assoluta di una gestione autonoma dei documenti informatici e della loro sicurezza, per preservarne la qualità ed il valore sia dal punto di vista tecnico sia dal punto di vista giuridico.

---

[180] Da un punto di vista teorico, simmetricamente a quanto esaminato in senso generale, l'enunciazione delle funzioni notarili può essere realizzata:

senza alcun accorgimento tecnico, ma attraverso un'autorità di certificazione propria del Notariato, la cui principale politica, resa nota ed impegnativa attraverso il Manuale Operativo, consista nel rilascio di firme elettroniche esclusivamente a notai in esercizio, e da utilizzarsi esclusivamente per attività svolte nell'esercizio delle funzioni notarili;

attraverso diverse autorità di certificazione, che rilascino certificati di firma ai notai, che siano dedicati all'esercizio delle funzioni notarili enunciate attraverso le estensioni standard del certificato, ed il cui ciclo di vita sia in ogni caso sotto il controllo, per quanto di competenza, del Presidente del Consiglio Notarile;

attraverso il rilascio, a cura dei Consigli Notarili, ma utilizzando una struttura necessariamente convergente verso il Consiglio Nazionale del Notariato, di certificati di attributo che attestino la sussistenza delle funzioni, il cui ciclo di vita sia esclusivamente sotto il controllo del Consiglio Notarile Distrettuale, e che siano collegati, ma non in modo indissolubile, a certificati di firma rilasciati da un qualunque certificatore alla persona fisica che, attraverso solo il certificato di attributo, riveste e dichiara il ruolo di notaio.

[181] P. PICCOLI ed U. BECHINI, Documento informatico, firme elettroniche e firma digitale (in AAVV, Diritto di Internet e dell'E-Business, Collana Diritto delle nuove tecnologie, Milano 2003)

Il tutto in uno scenario molto variegato, in cui la competenza tecnologica non sempre va di pari passo con la cultura del documento giuridico, dei suoi usi e della sua conservazione, e nel quale la mancanza di esperienze diffuse rende prevedibile che gli autori delle prime applicazioni di successo possano essere i capofila del processo di pratica del documento informatico.

La realizzazione del notariato italiano presenta quindi vantaggi di carattere operativo ed, in senso lato, politico, consentendo di partecipare in modo attivo alla realizzazione dei processi. In linea di principio, nulla si oppone all'utilizzo di queste tecniche, e soprattutto di questo tipo di approccio attivo, anche in ambito internazionale. Già dalla fine del 2002 la firma di un qualunque notaio italiano può essere verificata da chiunque nel mondo, utilizzando le risorse liberamente disponibili su Internet all'indirizzo http://ca.notariato.it. Nel giro di una manciata di secondi, qualunque utente della Rete può così ricevere l'assicurazione che un determinato documento digitale proviene da un notaio italiano nel pieno esercizio delle sue funzioni. Se, come è negli auspici dell'UINL, tale sistema sarà adottato da tutti i notariati del mondo, saranno disponibili gli strumenti per un'agevole ed istantanea circolazione telematica del documento notarile, a pieno valore legale.

Perché tale obiettivo sia conseguito, occorre però che in alcuni ordinamenti (tra cui quello italiano) siano superate difficoltà d'ordine formale. E' il caso dei vincoli posti dagli ordinamenti che pretendono la legalizzazione dei documenti provenienti dall'estero, oppure la formalità sostitutiva (Apostille) prevista dalla Convenzione dell'Aja. L'Apostille, in particolare, è una formalità disciplinata in modo assai dettagliato nelle sue caratteristiche anche fisiche [182], che non pare possibile estendere con facilità al mondo informatico. Altri trattati internazionali, come la Convenzione di Bruxelles del 25 maggio 1987 [183], si limitano a sopprimere *tout court* la legalizzazione, e sono pertanto suscettibili di applicazione anche al documento con firma digitale. Si può anzi affermare che già allo stato attuale i documenti notarili provvisti di firma digitale possano liberamente circolare tra Italia e Francia, con pieno valore giuridico.

3. La durata del documento informatico

L'idea che un documento abbia una data di scadenza è estremamente familiare. Che si tratti di una carta di credito o di una procura, un fatto è costante: con la scadenza il documento diviene inidoneo a supportare la nascita di nuovi rapporti giuridici, ferma restando però la validità storica degli atti e dei rapporti sorti durante il periodo di validità del documento.

Nell'ambito della firma digitale le cose appaiono completamente diverse. E' stato affermato da più parti, non senza fondamento, che quando scade il certificato di firma digitale, tutti i documenti sottoscritti durante il periodo di validità della firma stessa perdono rilevanza giuridica. Scrive Raimondo Zagami [184] che la scadenza della firma produce un effetto corrispondente alla distruzione del documento. E la scadenza è eventualità tutt'altro che teorica, visto che la validità di un certificato correntemente non supera i tre anni. Sopravvive, s'intende, il fatto storico dell'avvenuta documentazione,

[182] La Convenzione dell'Aja del 5 ottobre 1961, che istituisce l'Apostille, si spinge, come è noto, sino a dettare forma e misura minima dell'Apostille medesima: *un carré de 9 centimètres de côté au minimum*.

[183] In vigore attualmente (primavera 2004) tra Belgio, Danimarca, Francia, Irlanda ed Italia.

[184] Firma digitale e sicurezza giuridica, Cedam, Padova 2000, p. 214

suscettibile di prova, ma il documento informatico in quanto tale sarebbe giuridicamente evaporato.

Questo fenomeno, prima facie sorprendente, è ancora di non consolidato inquadramento giuridico, ed alimenta perplessità di vario genere. Occorre però ammettere che la cosa appare perfettamente naturale sol che si ponga mente al meccanismo di produzione di una firma digitale [185].

Come si è già osservato, a rigore non è impossibile risalire dalla chiave pubblica a quella privata, usurpando la firma di chiunque altro: è solo un'operazione molto lunga e difficile. Ma quanto lunga? Occorre essere diffidenti. Nel 1977 serissimi scienziati stimavano che il miglior ritrovato di firma dell'epoca, noto come RSA129, richiedesse milioni di anni per essere violato [186]; un quindicennio più tardi ad un team di esperti bastarono appena sei mesi [187]. Simili sorprese non derivano solo dal costante incremento di potenza dei computers ma anche e soprattutto dallo sviluppo di tecniche di criptoanalisi che consentono di semplificare con vari espedienti l'inconcepibile mole di calcoli richiesta da un attacco matematico diretto. Da questo punto di vista l'impiego abituale della firma digitale aumenta i rischi: disponendo di molti esemplari di firma di un medesimo soggetto, è più facile per un potenziale pirata scoprire la chiave, che ovviamente è sempre la stessa.

Non si può pertanto escludere che tra cinque anni violare una delle chiavi attualmente in uso divenga un compito relativamente semplice. Se così fosse, nel 2009 chiunque potrà produrre un documento provvisto di una perfetta ed ineccepibile firma digitale di qualunque soggetto a sua scelta, datata 2004. E quindi i documenti sino a quel momento firmati con quella chiave cesseranno di essere affidabili, perché facilmente falsificabili. Questa è la ragione per cui si afferma che i documenti perdono rilevanza giuridica con la scadenza della relativa chiave di firma digitale, siano essi autenticati o meno: anche la firma digitale del notaio scade, come tutte le altre. Per conservare la piena validità del documento occorre insomma poter dimostrare la sua anteriorità alla data di scadenza del certificato di firma. Ma come?

La via maestra è l'apposizione della marca temporale, o *timestamping*. Espressione tecnica che in realtà cela un'operazione molto semplice: il documento viene trasmesso ad un certificatore, il quale lo restituisce con una menzione provvista di data e firma digitale. Se un documento è stato firmato nel 2004 con una firma che scade il 31/12/2006, è sufficiente sottoporlo a marca temporale entro la fine del 2006 per protrarne la validità. Ma non all'infinito: la marca temporale non è altro che una firma digitale, e quindi scade a sua volta, riproponendo i medesimi problemi. La validazione temporale deve quindi essere compiuta periodicamente.

Laddove si vogliano conservare nel tempo importanti quantità di documenti con firma digitale, mantenendone intatto il valore giuridico, si deve quindi fronteggiare una sfida organizzativa di proporzioni non trascurabili. La soluzione risiederà con ogni probabilità nella creazione di apposite infrastrutture, provviste di un certo livello di

[185] cfr. § 2.1.2, nota 6.

[186] M. GARDNER A New Kind of Cipher that would Take Millions of Years to break, in Scientific American, v.237, n.8, pp 120-124, August 1977.

[187] L'impresa fu compiuta nel 1993 da Derek Atkins, Michael Graff, Arjen Lenstra e Paul Leyland avvalendosi dell'aiuto di 600 persone e 1600 computer in 25 paesi diversi. Vedasi Steven Levy, *Crypto*, cit., p. 273

centralizzazione, in grado di eseguire le operazioni necessarie in modo altamente automatizzato.

Tuttavia tale strada non può considerarsi esclusiva, ancorché consigliabile. L'estrema macchinosità, la mancanza di tecnologie diffuse che utilizzino la marcatura temporale, la pratica del documento informatico anche in assenza di tali accorgimenti lasciano prevedere che la prassi e la giurisprudenza si incaricheranno di individuare modalità aggiuntive ed alternative di verifica del tempo del documento.

La legislazione italiana, accanto alla marcatura temporale come sistema di validazione temporale e di opponibilità ai terzi[188], prevede già l'accertamento (ancorché senza un riconosciuto valore di opponibilità) del tempo del documento attraverso il riferimento temporale, inteso come semplice apposizione della data e dell'ora al documento[189].

Non va poi dimenticato che il sistema giuridico prevede alcuni sistemi certi per la determinazione del tempo del documento (la registrazione, l'autentica, la morte del sottoscrittore) che sia pure con gli adattamenti dovuti al fenomeno, non possono essere considerati del tutto inapplicabili alla pratica del documento informatico.

In conclusione può facilmente prevedersi che il giudice, chiamato a decidere, utilizzerà tutti gli elementi disponibili per la definizione del tempo del documento, indipendentemente dalla presenza della marcatura temporale.

Non va poi dimenticato che, una volta conservato il documento, deve assicurarsene la leggibilità nel tempo, il che tra l'altro impone il ricorso esclusivo a pochissimi formati non proprietari, ad amplissima diffusione [190], di cui garantire nei decenni [191] la leggibilità da parte delle piattaforme informatiche che verranno via via introdotte. Obiettivo meno banale di quanto sembri, e che richiederà probabilmente costante attenzione all'ininterrotta disponibilità di softwares capaci di interpretare tutti i formati, anche se fuori uso da decenni.

3.1 - La verificabilità nel tempo

L'operazione di *timestamping* può rivelarsi di fondamentale importanza anche sotto un altro profilo, di cui l'esperienza pratica italiana ha già posto in evidenza la rilevanza pratica. E' il caso, tra gli altri, della cessazione del notaio dall'esercizio. Negli ultimi giorni di permanenza in carica egli curerà tutte le formalità relative ai suoi atti; il suo certificato di firma sarà revocato con la cessazione dall'esercizio. Può darsi che alcune formalità non vengano esaminate immediatamente, ed il controllo sia eseguito quando il notaio è già cessato dalle sue funzioni [192]. Un'operazione di verifica informatica della firma apposta dal notaio darà come risultato quella di firma invalida in quanto apposta in base ad un certificato revocato. Un *timestamping* apposto prima dell'invio del documento [193], attesta invece, a livello informatico, l'anteriorità della

[188] art. 22 D.P.R. 445/2000, D.P.C.M. 13/1/2004.

[189] Art. 1 Deliberazione C.N.I.P.A. 11/2004, Art. 1 D.M. 23/1/2004.

[190] Come già rammentato, i notai italiani utilizzano esclusivamente i formati pdf ed xml.

[191] E' tutt'altro che scontato, ad esempio, che si riesca oggi a leggere con facilità i testi prodotti da un word processor di appena venti anni fa.

[192] Ciò è effettivamente accaduto per atti costitutivi o modificativi di società, trasmessi al Registro delle Imprese italiano, che esegue ancora un vaglio manuale delle formalità sottopostegli.

[193] Servizio che le Certification Authorities, compresa quella del notariato italiano, erogano correntemente.

firma rispetto alla revoca del certificato, consentendo alla verifica di svolgersi con esito positivo.

E' ben vero che, nella quasi totalità degli ordinamenti (e quello italiano non fa eccezione) la data apposta dal notaio fa piena prova, ma ciò non risolve il nostro problema. L'eventuale data apposta in calce al documento firmato, infatti, fa piena prova solo dopo che il documento informatico sia stato riconosciuto come un valido documento proveniente da notaio in esercizio: la revoca del certificato impedisce per l'appunto questo passaggio, che si situa ad un livello logico antecedente.

4. La firma digitale: un pericolo per il notariato?

Si è già posto in evidenza come qualunque tentativo di attribuire al documento digitalmente sottoscritto dal privato, senza intervento del notaio, lo stesso valore giuridico del documento autentico, sia del tutto privo di fondamento [194]. La constatazione è talmente ovvia da non meritare qui approfondimento. Ciò non toglie che gli strumenti informatici rappresentino senza dubbio una temibile sfida sotto altri punti di vista.

E' innanzitutto una sfida *politica*, che si colloca peraltro in un quadro più generale: qualora il notariato non sapesse adeguarsi all'uso degli strumenti che la tecnologia propone, si autocondannerebbe ad essere presto accantonato come istituzione incapace di servire i reali bisogni della società.

E' poi una sfida *professionale*. Il notariato non può rinunciare alla propria funzione, che è quella di produrre documenti a valore giuridico della più elevata affidabilità, in quanto derivanti dall'attenta indagine della volontà delle parti, dalla consulenza loro garantita per il miglior raggiungimento dei propri obiettivi, dall'attività di documentazione precisa ed imparziale, dalla conservazione nel tempo del documento stesso. Tradire tale funzione abbassandosi al ruolo di semplice gestore di flussi documentali generati altrove [195], senza un interazione diretta con le parti, significherebbe commettere un errore se possibile ancora più grave: rendersi inutili non in quanto obsoleti, ma in quanto incapaci di fornire il valore aggiunto proprio ed esclusivo della nostra attività. In nessun caso potremo transigere sui valori che fondano l'autorevolezza dell'atto notarile, e lo collocano da sempre al vertice delle gerarchie delle prove.

Occorre però che il singolo notaio sappia controllare attivamente, e non subire, le tecnologie che il progresso pone a sua disposizione. Occorre che il notariato, a livello nazionale come internazionale, sappia definire e difendere gli standard (anche tecnologici) necessari a garantire che al mutamento del supporto (dalla carta al bit) non si accompagni scadimento alcuno della qualità della funzione.

Se non perderemo di vista questi obiettivi, potremo continuare a guardare al documento informatico, in tutta serenità, come ad un semplice strumento aggiuntivo a disposizione della nostra professione.

---

[194] Retro, § 2.2.2.1.

[195] E' il rischio latente nel profilo del cosiddetto Cybernotary, almeno quando lo si intenda (come talora si è fatto) quale mero garante del buon funzionamento del sistema di firma digitale, e non della corretta formazione di ogni singolo documento.

CAPITOLO IV

LE APPLICAZIONI NOTARILI

SOMMARIO. 1. Software e norme; 2. La pubblicità immobiliare; 3. Pubblicità commerciale.

1. Software e norme

Pervenire alla trasmissione di atti in forma digitale dal notaro ai Pubblici Registri istituzionalmente preposti è certamente soluzione assai interessante per il notariato. Una volta superata l'iniziale fase di adattamento, si conseguono importanti risparmi di tempi e di costi, ed è possibile operare in modo del tutto indifferente in qualunque parte del territorio interessato dal sistema. Già oggi, per un notaio italiano, non vi sono differenze rilevanti, sul piano organizzativo, nel ricevere la vendita di un immobile sito nella medesima città oppure a mille chilometri di distanza. Il notaio è posto in grado di fornire un servizio assai più efficiente, con evidenti ritorni positivi anche sul piano dell'immagine della categoria. Le Amministrazioni pubbliche, che ricevono i dati di cui hanno bisogno in modo rapido, semplice ed economico, sono inoltre spontaneamente condotte ad un maggior apprezzamento del ruolo del notaio, che diviene dal loro angolo visuale un partner difficilmente rinunziabile.

Una trasmissione rapida ed economica non è però che uno degli aspetti della questione. L'accesso telematico ad un archivio (in input e/o in consultazione) non è di per sé una soluzione del problema pubblicitario: il sistema informatico cui si accede deve possedere alcune qualità intrinseche. Deve essere consultabile in modo semplice e sicuro, così da pervenire senza eccessive complicazioni all'acquisizione dei dati che interessano all'ispezionante. Deve nel contempo fornire un quadro completo ed aggiornato della situazione giuridica di cui si opera la verifica, senza perdita di contenuti giuridicamente rilevanti. Questi obiettivi non sono agevolmente conseguibili, e sono anzi tra loro in qualche modo in conflitto.

Da un lato, infatti, la consultazione della base dati è tanto più agevole quanto più rigida è la sua organizzazione [196]. D'altro lato un'eccessiva rigidità può comportare la difficoltà (quando non l'impossibilità) di rendere percepibile all'ispezionante le effettive peculiarità giuridiche e le sfumature del singolo caso [197].

L'esperienza italiana in questo campo data a circa un ventennio or sono, quando venne intrapresa la meccanizzazione dei Registri Immobiliari. Il notaio si trovò di fronte alla necessità di rappresentare il contenuto del suo atto avvalendosi solo di un numero predeterminato di opzioni predefinite dall'Amministrazione. Sotto alcuni profili si trattò soltanto di adeguare alcune prassi ed abitudini consolidate. Probabilmente questo ebbe anche effetti positivi: in alcuni casi la pubblicità eseguita in linguaggio naturale consentiva al notaio di non prendere posizione sulle effettive caratteristiche giuridiche dell'atto ricevuto, ma di conservare un certo margine di vaghezza se non di ambiguità; approccio assai confortevole di fronte a fattispecie di non certissima qualificazione. La

[196] F. BROCHU, The Internet's Effect on the Practice of Real Property Law: A North American Perspective, 2003 (2) in The Journal of Information, Law and Technology (JILT). <http://elj.warwick.ac.uk/jilt/03-2/brochu.htm>.

[197] A. GALLIZIA, Conservatorie ed informatica (osservazioni di un utente), in Rivista del Notariato, 1992, p. 447

necessità di riempire in modo univoco un determinato campo del tracciato informatico obbligò ad assumere la responsabilità di una scelta: in qualche modo l'informatica costrinse il notaio a fare il notaio sino in fondo. Ma in alcuni casi (fortunatamente rarissimi, molto più rari di quanto sulle prime si temesse) il sistema pose in evidenza vere lacune: per difetto di concezione del software alcuni atti risultavano non correttamente pubblicabili [198].

Non si tratta di un semplice problema operativo o di aggiornamento dei softwares. Così ragionando si banalizzerebbe il problema: vi è una questione più profonda. Se una determinata scelta compiuta in sede di creazione del software impedisce di dare pubblicità (e quindi: di opporre ai terzi) un certo fatto giuridico, ciò vuol dire che il software viene ad assumere, che lo si voglia o meno, una funzione sostanzialmente normativa [199]. Con ciò facendo insorgere questioni importanti, talora di rango costituzionale. Chi approva il software? Con quali controlli? Come il reale contenuto del software è reso conoscibile ed accessibile al cittadino?

Il notariato italiano ha tentato di arginare tale problematica (non si può onestamente parlare di soluzione) reclamando un ruolo di primo piano nella costruzione dei sistemi informatici. Tale contributo non ha sempre avuto modo di esplicarsi in modo sempre del tutto soddisfacente, ma nel complesso il bilancio, dopo circa un anno di funzionamento a regime, appare positivo.

Ma vi è di più: l'intervento del notaio nella fase organizzativa e progettuale delle nuove procedure della pubblicità consente di renderne il contributo al funzionamento generale del sistema sempre meno esterno al sistema e sempre più integrato nello stesso, con ciò rendendosi più necessario il ruolo del notaio per fini che non riguardano più soltanto il regolamento dei rapporti interprivatistici, ma per la realizzazione di finalità di interesse pubblico, quali quella della tenuta dei pubblici registri immobiliari e commerciali.

2. La pubblicità immobiliare

Si è già accennato in precedenza [200] alla realizzazione di un sistema sperimentale che consente la trasmissione dei dati relativi al pagamento dell'ICI (Imposta Comunale sugli Immobili) evitando ai cittadini che acquistano o vendono un immobile la necessità di adempimenti amministrativi (la presentazione della denuncia al comune competente da parte di acquirente e venditore) spesso onerosi, e garantendo all'ente pubblico interessato un corretto e tempestivo aggiornamento degli archivi, che facilita l'imposizione e riduce al minimo le fasi di controllo e verifica. Ciò è stato possibile, e sarà esteso in futuro a tutto il territorio nazionale, grazie ad un'iniziativa del notariato che rende disponibili a tali fini, in modo non oneroso per i singoli notai, i dati contenuti negli atti notarili, ed utilizzati per l'adempimento degli obblighi tributari strettamente connessi all'atto notarile, mediante la procedura detta dell'Adempimento Unico Informatico.

L'Adempimento Unico Informatico è il meccanismo giuridico e tecnologico attraverso il quale i notai italiani procedono alla registrazione ed alla esecuzione delle formalità immobiliari relative alla pubblicità immobiliare in senso proprio (trascrizione,

[198] A. MARZOCCHI, Il caso Grosseto, in Rivista del Notariato 1998, p. 795
[199] A. GALLIZIA, Problemi d'informatica notarile, in Rivista del Notariato, 1998, p. 10
[200] Cfr. supra § 1.3.

iscrizione ipotecaria, annotamenti) ed all'aggiornamento dei registri catastali. Questo sistema è obbligatorio per tutti gli adempimenti relativi agli atti di compravendita e per talune categorie di atti meno ricorrenti, e sarà esteso nel corso dell'anno 2004 a tutti gli atti immobiliari. E' anche previsto che una modifica normativa consenta l'estensione di tale modalità alla registrazione di tutti gli atti non immobiliari, operazione in verità semplicissima in quanto si tratta di atti che presentano problematiche applicative, sia dal punto di vista tecnico, sia da quello giuridico del regime tributario, molto minori di quelle finora affrontate e risolte.

Poiché già il primo approccio descrittivo ha evidenziato alcune delle contraddizioni genetiche del sistema, occorrerà fare una breve storia della nascita di questa procedura la quale, pensata, progettata, e scritta (anche dal punto di vista normativo) nel corso dell'anno 1999, risente da una parte della sua genesi e del sistema preesistente, dall'altra delle evoluzioni tecnologiche e normative intervenute dal momento in cui è stata pensata.

I notai italiani sono, sin dall'unità nazionale (1861), responsabili nei confronti dello stato delle imposte indirette dovute allo stato in sede di assolvimento dell'obbligo di registrazione. L'imposizione sugli atti notarili è talmente connaturata all'attività del notaio da costituire materia di esame al concorso per la nomina a notaio, e la consulenza al cliente in questo settore è talmente insita nell'attività notarile da costituire, secondo la giurisprudenza italiana, attività obbligatoria del notaio.

Tuttavia l'intero sistema era basato su un'attività di controllo preventivo, e la liquidazione delle imposte era quindi effettuata dall'ufficio tributario al momento della registrazione. Analogo era il sistema previsto per l'esecuzione delle formalità relative alla pubblicità immobiliare ed al catasto. L'esigenza in questo secondo caso, essendo molto minore l'impatto fiscale, è quella di verificare l'astratta idoneità dell'atto a costituire fonte della pubblicità. In tutti i casi quindi, era prevista la presentazione di una richiesta (sia essa la richiesta di registrazione, la nota di trascrizione o iscrizione, o la domanda di voltura catastale) ad organi della Pubblica Amministrazione per l'esecuzione di formalità destinate a completare la valenza verso i terzi degli atti notarili, e ad assolvere obblighi di leggi. Da notare anche che la competenza per l'esecuzione di tali formalità spettava, e spetta, a differenti uffici della Pubblica Amministrazione.

La telematizzazione delle procedure non poteva quindi prescindere dal sistema di partenza, dalla sua organizzazione, e dalle risorse e tecnologie disponibili.

Una serie di vincoli normativi e tecnologici ha fatto sì che l'adempimento unico partisse in modo graduale, e che fosse posposta la totale telematizzazione delle procedure relativamente alla parte di maggior rilievo in tema di pubblica fede, e quindi di attività notarile, quella della pubblicità immobiliare, la cui esecuzione, nel sistema del codice civile italiano, è condizione di opponibilità ai terzi.

Il sistema dell'adempimento unico nasce sulla base di una legge delega e di una serie di provvedimenti normativi di attuazione *a cascata* di rango normativo via via inferiore e contenenti di conseguenza disposizioni sempre più tecniche e dettagliate[201].

[201] Il comma 134 lettera G) dell'art. 3 della legge 662/96 prevedeva infatti nella sua prima formulazione il trasferimento di tutte le competenze relative agli atti immobiliari agli uffici del territorio, responsabili della pubblicità immobiliare. In attuazione dello stesso era stato emanato il D.Lgs. 463/97, che all'art. 2 regolamentava tale trasferimento. L'art. 7 della legge 448/98 ha modificato la formulazione originaria della normativa di delega, ed ha abrogato la norma attuativa di cui all'art. 2 del D.Lgs. 463/97, eliminando il trasferimento di competenze in materia di imposta di registro al Dipartimento del Territorio,

Motivi riferibili al dettato normativo, ma ancor più all'organizzazione interna dell'amministrazione finanziaria hanno fatto sì che la prima applicazione del sistema riguardasse i soli atti immobiliari e che le formalità interessate, pur redatte dal notaio su un modello unificato, continuassero ad essere trattate dai tre distinti uffici delle Entrate (per la parte relativa all'imposta di registro e assimilate) del Servizio di Pubblicità Immobiliare, e del Catasto. Altro vincolo che non è stato possibile superare è quello relativo è l'assoluta immodificabilità, sulla base del contenuto della legge delega, della normativa civilistica in materia ipotecaria.

Ciò ha comportato limitazioni nell'emanazione delle norme di riforma, e la necessità pratica, per l'esecuzione delle formalità ipotecarie, della presentazione del titolo ancora cartaceo (e quindi della copia dell'atto pubblico o della scrittura privata conservata nella raccolta del notaio) presso il competente Ufficio dei Registri Immobiliari.

Questa situazione non era modificabile sulla base delle norme di delega. Tuttavia il legislatore era già intervenuto altrimenti legittimando in via generale l'uso del documento elettronico in luogo di quello cartaceo, con valenza quindi anche nel settore della pubblicità immobiliare, come si è esposto in altra parte di questo lavoro[202]. Il secondo comma dell'art. 15 della legge 59/97 (Bassanini) prevede infatti l'equiparazione del documento elettronico a quello cartaceo, senza limitazioni di sorta, a condizione che il documento elettronico soddisfi i requisiti previsti. E' stata quindi sancita espressamente (oggi dagli artt. 6 e 20 del T.U. 445/2000) la totale equiparazione delle copie elettroniche degli atti pubblici alle copie cartacee, purché siano munite della firma digitale del pubblico ufficiale, apposta in modo conforme alle disposizioni normative[203]. La normativa consente quindi di procedere alla esecuzione di formalità ipotecarie per via telematica, purchè i documenti trasmessi soddisfino i requisiti richiesti per il documento elettronico e siano muniti di valida firma digitale.

Poiché al momento dell'emanazione delle norme sull'adempimento unico non era ancora attiva un'applicazione di firma digitale a norma di legge, l'impianto normativo del regolamento attuativo (D.P.R. 308/2000) previsto dal D.Lgs. 18 gennaio 2000 n. 9 ha indicato di fatto due soluzioni per l'esecuzione delle formalità ipotecarie:

- la prima, già attuata, consente la trasmissione telematica della nota per la pubblicità immobiliare unitamente a tutti i dati occorrenti per la registrazione (contenuti nel modello dell'adempimento unico e con acclusi il testo dell'atto, ed i dati necessari per l'applicazione di particolari regimi tributari, in sostituzione dell'esibizione di certificazioni sinora in taluni casi prevista), ma subordina l'esecuzione della formalità alla presentazione del titolo cartaceo;

- la seconda, da attuarsi in un secondo tempo, in modo totalmente telematico, mediante la trasmissione di copie conformi elettroniche unitamente al modello dell'adempimento unico, e fermo restando il controllo riservato al conservatore per l'accettazione delle formalità.

---

e mantenendo quindi inalterate le competenze del Dipartimento delle Entrate. Sulla base dell'ultima formulazione della legge delega è stato emanato il D.lgs n. 9 del 18 gennaio 2000, che ha introdotto gli articoli da 3 bis a 3 sexies nel D.lgs 18 dicembre 1997 n. 463, e ha previsto un dal regolamento delegato emanato con D.P.R. 18.8.2000 n. 308, e poi un decreto interministeriale (Decreto Direttoriale 13 dicembre 2000), ed i successivi provvedimenti di attivazione della procedura per categorie di atti ed aree geografiche.

[202] Cfr § 2.1.1 e seguenti.

[203] Cfr. § 3.1.

Ad oggi è ancora attiva esclusivamente la prima modalità, con una modifica solo apparentemente di dettaglio. L'invio telematico delle formalità è effettuato dai notai previa apposizione della firma digitale. I notai inviano (*rectius* possono inviare [204]) quindi una documentazione perfettamente idonea a sostituire la documentazione cartacea anche ai fini della pubblicità immobiliare.

La procedura resta tuttavia vincolata al cartaceo per diversi ordini di ragioni:

- la mancata distribuzione ai responsabili degli uffici delle firme digitali che consentirebbero l'emissione dei documenti, normativamente previsti, che attestino l'avvenuta esecuzione delle formalità;

- la mancanza di un sistema che consenta l'archiviazione con sufficienti garanzie di conservazione nel tempo dei documenti informatici costituenti titolo per le formalità ipotecarie;

- la difficoltà di gestire un sistema di accettazione delle formalità promiscuo, in parte cartaceo ed in parte informatico, necessario fin quando gli altri utenti del sistema (altri pubblici ufficiali roganti, uffici della Pubblica Amministrazione, uffici giudiziari, avvocati ed ufficiali giudiziari) non saranno, come i notai, attrezzati per l'uso del documento informatico e della firma digitale, problema questo che può essere risolto solo con un intervento normativo;

- la presenza di norme del codice civile, e della legge che regola il servizio ipotecario[205] (legge 52/1985), che presuppongono, a volte in modo implicito, l'esistenza del documento cartaceo e rendono impossibile l'uso del documento informatico senza la loro preventiva modifica [206].

La delicatezza del tema, il regime pubblicitario della proprietà immobiliare, e la sua importanza per il notariato, giustificano da una parte la prudenza nel proseguire su questa strada, peraltro inevitabile, dall'altra la pretesa del notariato italiano di contribuire alla definizione ed alla organizzazione di quello che sarà il sistema

[204] In realtà la struttura del sistema impedisce che la documentazione sia del tutto completa ai fini della pubblicità immobiliare. Il modello adottato, sulla base della norma del secondo comma dell'art. 2 del D.P.R. 308/2000, prevede l'indicazione, ma non l'inserzione, dei documenti allegati all'atto originario. La normativa del codice civile sulla pubblicità immobiliare costringe alla presentazione di copia dell'atto oggetto di pubblicità immobiliare completa di tutti gli allegati. La trasmissione non è quindi (almeno per gli atti muniti di allegati) completamente idonea, anche se nulla astrattamente impedirebbe ad un notaio di procedere a questa allegazione e di pretendere l'esecuzione della pubblicità immobiliare sulla base di un titolo informatico.

[205] La legge 52/1985 è l'attuale legge regolamentatrice del servizio ipotecario, ed è la normativa di base per la prima informatizzazione del servizio di pubblicità immobiliare. Va notata però la diversità della filosofia generale del sistema. La legge 52/1985 prevede infatti alcune norme per l'informatizzazione delle conservatorie dei registri immobiliari nella fase dell'immissione dei dati nel sistema. In poche parole, è la predisposizione della formalità che avviene su supporto informatico sulla base di programmi il cui uso è reso obbligatorio. Dal 1998 la presentazione delle formalità ipotecarie su supporto informatico è obbligatoria su tutto il territorio nazionale. Tuttavia il dato finale primario, sul quale si fonda la pubblicità e quindi l'opponibilità è sempre il documento stampato su carta che risulta dall'elaborazione.

[206] In particolare gli articoli 2664, 2678, 2680, del codice civile sulla trascrizione dei titoli, la conservazione della nota, e la tenuta del Registro Generale d'Ordine, documento quast'ultimo sul quale si basa il principio dell'opponibilità a terzi sulla base della priorità delle trascrizioni, e gli articoli 17, 20 e 21 della legge 52/1985, che presuppone l'esistenza di modulistiche cartacee, nonché la norma della medesima legge 52/1985 (art. 24) che prevede gli orari di apertura degli uffici dei registri immobiliari, modalità questa difficilmente compatibile con un sistema telematizzato. Un esame di tali problematiche in G.Arcella *L'uso della firma digitale per gli adempimenti. Modalità attuative.* in AA. VV. *Firme Elettroniche….* Cit. pag. 139 ss.

telematizzato. Abbiamo visto[207] che tale operazione è prevista tra gli obiettivi immediati della Pubblica Amministrazione. Il notariato partecipa ai lavori per definire le caratteristiche e le garanzie del nuovo sistema e per adeguare il contesto normativo.

Esaminiamo ora quali sono le modalità operative attive dell'adempimento unico, che consentono al notaio di interagire (fatta eccezione per i fenomeni patologici) in modo telematico con tutti gli uffici interessati, salvo l'ufficio dei registri immobiliari, con una notevolissima semplificazione delle procedure.

Il sistema per l'esecuzione delle formalità di registrazione, nonché per l'assolvimento degli obblighi tributari inerenti l'esecuzione di formalità ipotecarie, può delinearsi come segue, sulla base del D.Lgs. 18 gennaio 2000, n. 9, che inserisce nuove norme nel D.Lgs. 463/1997, del D.P.R. 308/2000, e del D.D. 13 dicembre 2000.

L'art. 3 bis del D. Lgs. 463/97 prevede che la registrazione telematica sia effettuata, in relazione ai soli atti immobiliari, mediante la trasmissione per via telematica del modello unico informatico, che comprende anche il contenuto delle note di trascrizione, iscrizione nonché delle domande di annotazione e della voltura catastale. Il modello comprende il prospetto degli allegati e dei documenti e dei certificati da presentare in virtù di disposizioni di legge o regolamentari, al fine dell'individuazione del regime impositivo, anche agevolato. Tutta la documentazione è conservata in originale presso il notaio.

Il termine per la richiesta di registrazione è stato aumentato da venti a trenta giorni, adeguandolo quindi al termine fiscale per l'esecuzione delle formalità ipotecarie. Tale prolungamento del termine è tuttavia di scarsa rilevanza pratica. Infatti le formalità di registrazione ipotecarie, e di voltura, nel caso di trasmissione telematica del modello unico informatico, "sono eseguite previo pagamento dei tributi dovuti in base ad autoliquidazione". Ciò comporta, per la necessaria unitarietà dell'adempimento, l'obbligo del pagamento di tutti i tributi, ivi compresa l'imposta di registro, anteriormente all'esecuzione delle formalità ipotecarie. E' ovvio quindi che permanendo la norma che obbliga il notaio, sotto la propria personale responsabilità, all'esecuzione immediata delle formalità di trascrizione (art. 2671 c.c.), il termine entro cui eseguire le formalità è in realtà inferiore a quello fissato ai fini fiscali, e comporta in molti casi la necessità di acquisire i fondi necessari per l'esecuzione della registrazione in anticipo rispetto alla data dell'atto. Tale modifica normativa ha comportato notevoli ricadute nell'organizzazione del lavoro e nel rapporto con la clientela, ma è stata necessaria per l'unificazione dell'adempimento.

Si è detto che il pagamento avviene sulla base dell'autoliquidazione effettuata dal notaio. In verità non può propriamente parlarsi di autoliquidazione, che è solo quella effettuata dal soggetto passivo dell'imposta. Come detto, il notaio nel sistema dell'imposizione indiretta e dell'imposta di registro in particolare, assume la figura di responsabile di imposta, e non sembra che le modifiche normative mutino tale situazione.

L'autoliquidazione tuttavia incide in modo sostanziale sulle modalità operative per la registrazione degli atti. E' infatti eliminato il controllo preventivo da parte dell'ufficio ed in conseguenza la possibilità di rifiuto della registrazione o dell'esecuzione di formalità ipotecarie. Ciò però nel solo caso di insufficiente versamento, non nel caso di omesso versamento. L'omissione di versamento dell'imposta, costituisce motivo di rifiuto delle formalità ipotecarie. La liquidazione, il

[207] Cfr § 1.3.

relativo pagamento, e la trasmissione del modello e degli altri documenti e dati in precedenza elencati, comportano l'esecuzione delle formalità di registrazione, ipotecarie e di voltura, salva la necessità, come si è visto, di effettuare la consegna del titolo cartaceo per le formalità ipotecarie.

Eseguite le formalità, l'ufficio rilascia ricevuta in forma elettronica e per via telematica ed è obbligo del notaio annotare gli estremi della registrazione sull'originale dell'atto. Parimenti gli uffici devono rendere disponibili le informazioni sulle imposte principali e sullo stato di esecuzione delle formalità a mezzo di un archivio elettronico.

Per quanto riguarda la certificazione di avvenuta esecuzione della formalità ipotecaria ed il duplo della nota di iscrizione, trascrizione o annotamento, il rilascio avverrà in forma cartacea sino a quando l'invio del titolo avverrà in forma cartacea.

La normativa in esame definisce poi le procedure per il controllo dell'autoliquidazione ed il recupero della maggiore imposta. Il meccanismo individuato si basa su una modifica normativa complessa, consistente essenzialmente nella concessione di un termine di trenta giorni per gli uffici per il controllo e nella modifica della definizione legislativa di imposta principale.

Infatti gli uffici controllano la regolarità dell'autoliquidazione e del versamento dell'imposta e, qualora risulti dovuta una maggiore imposta, nel termine di trenta giorni notificano un avviso di liquidazione anche per via telematica. Il pagamento è effettuato, entro quindici giorni dalla data della suindicata notifica; trascorso tale termine, sono dovuti gli interessi moratori e si applicano le sanzioni. Qualora gli uffici ravvisino dolo o colpa grave nell'autoliquidazione delle imposte segnaleranno le irregolarità agli organi competenti in materia disciplinare per l'applicazione delle sanzioni. L'unica norma sanzionatoria sembra qui essere, per i notai, l'art. 147 della legge notarile [208].

E' da dire che tale facoltà (ed in certi casi obbligo) degli uffici, inserita in una delle ultime stesure del decreto per evidenti scopi tuzioristici, non sembra pensata con un preciso riferimento a norme sanzionatorie quali l'art. 147 L.N., e non sembra creare i presupposti di un efficiente sistema sanzionatorio dal punto di vista disciplinare, a causa della genericità eccessiva della formulazione, che subordina anche il solo avvio di un'azione disciplinare alle determinazione di due diverse entità (ufficio e titolare dell'azione disciplinare).

L'ambito del controllo degli uffici è opportunamente circoscritto da due elementi normativi:

- in primo luogo il controllo degli uffici è effettuato "sulla base degli elementi desumibili dall'atto"; tale locuzione, che in verità si limita a ribadire la natura di "imposta d'atto" dell'imposta di registro, ha la funzione di chiarire che l'ufficio non è legittimato, a liquidare in questa sede, ed a richiedere quindi al pubblico ufficiale imposte diversa da quella principale; non potrà quindi verificarsi il caso che un ufficio effettui in questa sede l'accertamento di maggior valore degli immobili, o che sulla base di un controllo estrinseco revochi agevolazioni la cui concessione non è normativamente subordinata ad alcuna forma di controllo preventivo;

- in secondo luogo l'imposta liquidata e richiesta dall'ufficio entro il detto termine di trenta giorni dalla registrazione è espressamente qualificata come imposta principale, qualora sia diretta a correggere errori od omissioni effettuati in sede di autoliquidazione. E' evidente che gli errori e le omissioni riguardano non solo il calcolo, ma anche le

[208] Che prevede un ventaglio amplissimo di sanzioni, a seconda della gravità del comportamento, sino alla destituzione.

problematiche interpretative che sinora erano affrontate in sede di registrazione dell'atto. Tuttavia tale norma contribuisce a sua volta a delimitare il contenuto del controllo dell'ufficio, qualificando implicitamente quali imposte complementari o suppletive, e quindi al di fuori della responsabilità del pubblico ufficiale, tutte le fattispecie di imposizione successiva non risultanti da errori ed omissioni effettuati in sede di autoliquidazione.

Il pubblico ufficiale, in caso di notifica di avviso di liquidazione della maggiore imposta per il caso di errori od omissioni in sede di autoliquidazione, è senz'altro legittimato all'impugnativa, con ciò rinunciando al beneficio derivante dalla disposizione che esclude, nel caso di pagamento nei quindici giorni, che siano dovute sanzioni amministrative. Resta da definire se siano legittimati all'impugnativa o all'intervento le parti dell'atto, e quali possano essere i rapporti tra il pubblico ufficiale e le parti in questa ipotesi.

Accanto all'ipotesi di liquidazione e pagamento insufficiente si pone poi l'ipotesi di liquidazione e versamento eccessivo, nel qual caso è ammessa la compensazione con le imposte dovute per atti di data posteriore. Le modalità pratiche della compensazione risultano dal decreto relativo al modello unico, che prevede le modalità per l'indicazione della compensazione, dei precedenti atti di riferimento ed eventualmente delle ragioni della stessa.

L'ultima modifica legislativa di rilievo è quella relativa all'imposta di bollo. Per la stessa è previsto un pagamento in misura forfetaria cumulativa comprensiva dell'imposta di bollo relativa agli originali atti relativi a diritti sugli immobili sottoposti a registrazione con modalità telematiche, alle copie conformi per gli usi relativi all'esecuzione delle formalità di registrazione, ipotecarie e di voltura, ed alle formalità stesse. Tale norma risolve in modo forse rozzo, ma senz'altro efficiente, il problema della liquidazione dell'imposta di bollo per documenti non cartacei.

L'applicazione della procedura telematica non può infine avvenire senza la definizione delle modalità di pagamento, che devono essere adeguate al nuovo sistema. La soluzione prescelta è quella dell'addebito mediante RID presso istituti di credito convenzionati, avvalendosi di un sistema ormai adottato in via generalizzata in ambito tributario.

Il discorso sull'adempimento unico merita, in conclusione alcune notazioni di carattere generale. Molta attenzione abbiamo dedicato al procedimento di autoliquidazione. Ciò non è casuale: al di là delle peculiarità operative, l'introduzione delle procedure di autoliquidazione (e di compensazione) modifica un sistema derivante da un'esperienza plurisecolare, ed affidano al notaio compiti che sinora gli erano preclusi. Si trasferisce dallo Stato al Pubblico Ufficiale la competenza alla liquidazione dell'imposta, riservando al primo solo un potere (peraltro limitato) di controllo. Ciò semplifica il compito per la Pubblica Amministrazione e lo rende più gravoso, ma soprattutto più carico di responsabilità, per il notaio. Tuttavia non può non notarsi che l'aumento dei compiti costituisce nel contempo un'accresciuta rilevanza del ruolo del notaio, ed una conseguenza del fenomeno del progressivo ritiro dello Stato da attività che allo stesso erano state storicamente riservate. Il ruolo del notaio è quindi accresciuto dall'adempimento unico, e le attività del Consiglio Nazionale del Notariato in materia di informatica costituiscono anche un necessario supporto a tali funzioni.

Il Modello Unico è basato inoltre sullo XML, che è un formato di pubblico dominio, e dunque non proprietario. Questa caratteristica, che sino a poco tempo fa sarebbe stata considerata poco più che una curiosità per addetti ai lavori, assume oggi

un'importanza che non è esagerato definire strategica. Nel mondo della contrattazione immobiliare l'informatica è prevalentemente stata sino ad ieri un ausilio importante ma concettualmente fungibile. Con la presentazione dei documenti in forma elettronica l'informatica penetra sino al cuore stesso della funzione: i files trasmessi agli Uffici per gli adempimenti pubblicitari sono in diverse ipotesi il veicolo unico, e non più collaterale, del flusso documentale generato dai notai. Gli strumenti informatici debbono quindi essere sotto l'integrale controllo del suo utilizzatore, il che non è possibile, o comunque assai più arduo, quando lo strumento stesso appartenga in via esclusiva ad un determinato produttore commerciale. In tal caso infatti:

l'organizzazione dei formati proprietari è nota nei dettagli solo al produttore, il quale può dunque agevolmente occultare al suo interno una congerie di dati che non vengono tutti presentati in video all'utilizzatore. Capita assai di frequente che i softwares memorizzino automaticamente nei files elementi anche assai delicati [209], all'insaputa dell'utente di accortezza media od anche medioalta. Tali dati restano però rintracciabili dal produttore stesso e talvolta da un operatore solo un poco più esperto od attento. Laddove il file sia sottoposto a firma digitale, anche tali informazioni vengono ovviamente firmate, all'insaputa del sottoscrivente;

- non è sempre possibile eseguire senza il concorso della Casa produttrice i necessari adeguamenti del software alle esigenze sopravvenute;

- è per lo più necessario acquistare il software della Casa produttrice per produrre e lavorare con sicurezza i files;

- è possibile che in futuro sia reso necessario acquisire il consenso della Casa produttrice perché il software possa trattare determinati files o tipi di files [210].

Nulla di tutto questo accade utilizzando il formato xml, che è totalmente aperto, gestibile e programmabile utilizzando una pluralità di strumenti di pubblico dominio, il cui impiego non è sottoposto ad alcuna limitazione o controllo.

3. Pubblicità commerciale

Vicenda un poco diversa ha interessato la pubblicità commerciale. In Italia tutti gli atti costitutivi e modificativi di società commerciali di ogni tipo richiedono obbligatoriamente l'intervento notarile. Il sistema di pubblicità commerciale è stato profondamente rivisto nel 1993 [211], prevedendo un elevato grado di informatizzazione. Più tardi, tra il 2002 ed il 2003, è stato progressivamente introdotto l'obbligo di presentazione della documentazione in via telematica, con ricorso alla firma digitale. Questo obbligo interessa tutti gli utenti del sistemi, e quindi anche le società che eseguono l'annuale deposito del bilancio od altri minori adempimenti pubblicitari: si

[209] § 2.2.4.

[210] E' il caso del sistema Microsoft originariamente noto come Palladium, ma ritirato, almeno sotto questa denominazione, dopo furibonde reazioni a livello internazionale, di cui è stato alfiere nell'ottobre 2002 Richard Stallman, *Can you trust your computer?* http://www.gnu.org/philosophy/can-you-trust.html (anche in traduzione italiana, *Puoi fidarti del tuo computer?* in *Interlex*, 31/10/2002, http://www.interlex.it/675/stallman.htm). Secondo il progetto originario, per quanto è dato sapere a chi scrive, le macchine provviste dei futuri sistemi operativi della nota Casa americana si sarebbero rifiutate di trattare determinati files, scelti secondo parametri stabiliti dalla Casa stessa e probabilmente variabili nel tempo, con l'obiettivo dichiarato di reprimere la pirateria informatica. La questione ha innumerevoli risvolti, ma qui preme evidenziarne uno solo: resta difficile accettare l'idea che l'operatività di sistemi destinati all'esercizio di funzioni tipiche di uno Stato sovrano debba sottostare al placet di un'impresa privata, ed extracomunitaria per di più.

[211] Legge 29 dicembre 1993, numero 580.

tratta quindi di un sistema che coinvolge milioni di soggetti. I notai impiegano il sistema di firma digitale del Consiglio Nazionale del Notariato; tutti i restanti soggetti interessati usano quasi esclusivamente le smart cards rilasciate da Infocamere, l'operatore informatico delle Camere di Commercio.

Il funzionamento del sistema, per quanto concerne gli atti notarili, è a grandi linee il seguente. Gli atti vengono dapprima convertiti in formato pdf, operando direttamente dal word processor od attraverso uno scanner, od anche impiegando promiscuamente le due tecniche. A parte si prepara una modulistica, secondo modelli approvati dal competente Ministero. Atto e modulo d'accompagnamento sono sottoscritti digitalmente dal notaro, ed entrambi inoltrati in via telematica impiegando un software apposito.

Le questioni giuridiche che il funzionamento del sistema pone sono molte e talvolta assai delicate nei loro riflessi pratici [212], ma originano per lo più da dettagli del sistema normativo. Un problema di più ampia portata è invece costituito dalla documentazione delle fasi successive dell'iter. Il sistema è ancora insoddisfacente sotto vari aspetti ed in via di perfezionamento, e gli obiettivi cui tendere sono ben nitidi.

Il notaio, che ha gravi responsabilità, deve innanzitutto disporre di una prova indiscutibile dell'avvenuta esecuzione delle formalità di sua responsabilità [213]. Le operazioni pubblicitarie debbono poi essere evase con rapidità e nel rispetto dell'ordine di presentazione: qui è invece l'interesse pubblico ad una corretto funzionamento del sistema ad assumere un ruolo preminente. Il controllo da parte dell'Amministrazione deve altresì essere conforme a standard predeterminati, conoscibili e pienamente conforme a legge; l'eventuale rifiuto di esecuzione della formalità deve essere portato a conoscenza delle parti interessate in tempi e modi certi.

[212] Vedasi l'esauriente trattazione di Gea ARCELLA, L'uso della firma digitale per gli adempimenti: modalità attuative, in AAVV, Firme elettroniche: questioni ed esperienze di diritto privato, Giuffrè, Milano 2003

[213] Che non sembra poter consistere in nulla di diverso da una ricevuta digitalmente firmata dall'Amministrazione.

Nota bibliografica

Nella letteratura specialistica italiana, e limitandosi ai contributi apparsi in volume, sono numerosi i contributi di notai su questo argomento, a cominciare dalla pioneristica ed autorevolissima trattazione di Mario MICCOLI, *Documento e Commercio Telematico*, IPSOA, Milano 1998.

Il testo più ampio è quello di Raimondo ZAGAMI, *Firma digitale e sicurezza giuridica*, Cedam, Padova 2000. Si ricordano inoltre:

Paolo PICCOLI e G. ZANOLINI, Il documento elettronico e la «firma digitale», *Rivista del Notariato*, 2000, 879, anche ne *I problemi giuridici di Internet*, a cura di TOSI E., contributi di BARBARISI M., BUONOMO G., CERINA P., FINOCCHIARO G., PICCOLI P., TOSI E., TOSI T. e ZANOLINI G., Giuffrè, Milano, 1999, di cui è apparsa nel 2003 un'edizione aggiornata con il contributo di Ugo BECHINI;

M. CAMMARATA ed Enrico MACCARONE, *La firma digitale sicura*, Giuffré Milano 2003;

Enrico SANTANGELO e Michele NASTRI, *Firme elettroniche e sigilli informatici*, p. 1133, in AAVV, *Diritto dei consumatori e nuove tecnologie*, Giappichelli, Torino 2003; e su *Vita Notarile*, 2003/2.

Da ultimo, ad opera di sei notai (Gea ARCELLA, Ugo BECHINI, Sabrina CHIBBARO, Marco DOLZANI, Michele NASTRI e Raimondo ZAGAMI) è apparso nella Collana Studi del Consiglio Nazionale del Notariato il volume *Le firme elettroniche (Questioni ed esperienze di diritto privato)* Giuffré, Milano 2003.

Posizione peculiare, assai distante da quella seguita nel presente lavoro, quella di Andrea BORTOLUZZI, voce *Forma Telematica* dell'aggiornamento al *Digesto Quarto*, Discipline Privatistiche, Sezione Civile, UTET, Torino 2002.