

# Vademecum minimo in tema di Funzione notarile e firma digitale

(\*)

Definitivo – 1 giugno 2000

ugo bechini - [ubechini@notariato.it](mailto:ubechini@notariato.it)

Facile, facilissimo. Apporre una firma digitale è quel che si dice un gioco da ragazzi. Si introduce una tessera, detta *smart card*, nell'apposita fessura, si digita una *password*, si premono pochi altri pulsanti ed è fatta. Non è più complicato di un prelievo Bancomat. Un utilizzo consapevole del mezzo, che tenga conto delle sue implicazioni tecniche e giuridiche, è evidentemente un altro discorso.

Dalla firma digitale si richiedono fondamentalmente due cose: l'attestazione della provenienza della dichiarazione, cui nella realtà cartacea provvede la sottoscrizione, e la non alterabilità del suo contenuto. La soluzione ormai standard a livello mondiale consiste nell'uso di un sistema crittografico, proposto nel 1975 da Whitfield Diffie e Martin Hellman, e portato poi a maturità nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman <sup>1</sup> con la tecnica detta, dalle loro iniziali, RSA: la crittografia a chiavi asimmetriche. Per comprendere il nesso che lega la crittografia asimmetrica alla sottoscrizione digitale converrà prendere le mosse dalla tradizionale crittografia a chiavi *simmetriche*.

La crittografia simmetrica è ben nota a tutti fin dai banchi delle scuole elementari. Pensiamo al "sistema" che utilizza come chiave la sostituzione di ogni lettera con quella che immediatamente la precede nell'ordine alfabetico: ad esempio "Ibm" diviene "Hal" <sup>2</sup>. 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.

Nei sistemi a chiavi asimmetriche invece l'utilizzatore produce, avvalendosi di un software di semplicissimo utilizzo <sup>3</sup>, 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 <sup>4</sup>. Un testo criptato con la chiave pubblica può

<sup>1</sup> Ronald L. Rivest, Adi Shamir, Len Adelman, *On Digital Signatures and Public Key Cryptosystems*, MIT Laboratory for Computer Science Technical Memorandum 82 (April 1977).

<sup>2</sup> Così si chiamava, non a caso, il supercomputer ribelle di *2001 Odissea nello spazio*

<sup>3</sup> Come il celebre PGP (Pretty Good Privacy) di Philip Zimmermann, liberamente reperibile su Internet. L'efficacia del software è tale da aver provocato all'Autore non pochi guai con la giustizia americana. Per la legislazione di quel Paese i prodotti per crittografia sono infatti considerati a rilevanza militare: persino per softwares ad enorme diffusione come Netscape, che incorporano blande funzioni crittografiche, vige un teorico divieto di esportazione verso Paesi come Siria e Libia. La posizione americana appare ormai alquanto velleitaria, sia alla luce della pratica impossibilità di controllare la circolazione di un software, sia perché esistono prodotti non americani di equivalente efficacia; d'altronde neppure lo RSA può dirsi un'esclusiva americana visto che Shamir, secondo nome in ditta, è cittadino israeliano. PGP funziona, se non si ha troppa fretta, persino sui vecchi computers della generazione 286 (metà anni Ottanta): questo perché la sicurezza del sistema non riposa su fantascientifiche diavolerie elettroniche, ma su proprietà puramente matematiche note e studiate da molti decenni.

<sup>4</sup> Il sistema RSA si basa principalmente sul procedimento di fattorizzazione, ossia la scomposizione di un numero in numeri primi. Se è ovvio che  $21 = 3 \times 7$ , è meno elementare scoprire che  $92648497 = 12157 \times 7621$  (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  $12157 \times 7621$ , viene invece compiuta in una frazione di secondo dalla più economica delle calcolatrici tascabili ad otto cifre, del tipo che si trova nelle uova di Pasqua. 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. I sistemi asimmetrici sono vulnerabili (dal punto di vista matematico) sotto un duplice profilo. Primo: un procedimento matematico di fattorizzazione oggi non esiste ma non è a rigore escluso che venga scoperto in futuro; eventualità peraltro improbabile, dato che alcuni tra i migliori matematici del mondo vi stanno lavorando da circa un secolo. Secondo: per ciclopico che sia il compito, è

essere letto soltanto se si possiede la relativa chiave segreta. La chiave segreta deve essere accuratamente custodita <sup>5</sup>, quella pubblica può, ed anzi in un certo senso deve, essere diffusa il più possibile, senza alcuna precauzione: tipicamente, questa è depositata in archivi liberamente accessibili a chiunque via Internet.

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 resta sulla *smart card* di Caio, e non deve essere comunicata a chicchessia.

La stessa tecnologia può essere impiegata per la sottoscrizione nel modo seguente. Il testo <sup>6</sup> da inviare resta in chiaro, leggibile per chiunque. Il medesimo testo viene pure criptato avvalendosi della chiave segreta del sottoscrittore; il messaggio in cifra che ne deriva è appunto la firma digitale, e viene acclusa al testo in chiaro <sup>7</sup>. 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 <sup>8</sup>. Il destinatario, o qualunque soggetto comunque interessato, procuratosi la chiave pubblica del mittente, confronta messaggio e firma digitale. Se il confronto dà esito positivo, due

---

possibile violare le chiavi per tentativi, utilizzando la *brute force* dei calcolatori elettronici. Anche i più potenti supercomputers hanno però bisogno di molto tempo. Quanto è difficile dire, ed è certamente prudente diffidare di stime troppo roboanti: quando nel 1993 Derek Atkins, Michael Graff, Arjen Lenstra e Paul Leyland riuscirono in pochi mesi a violare il cosiddetto RSA-129, avvalendosi dell'aiuto di 600 persone e 1600 computer in 25 paesi diversi, poterono a buon diritto affermare di aver portato a termine il compito con mille anni di anticipo sul previsto! Una chiave a 512 bit è stata violata da un team di matematici nell'agosto 1999; le chiavi attualmente in uso per applicazioni professionali sono però di almeno 1024 bit. Esistono poi tecniche crittografiche che potrebbero semplificare il compito: se ad esempio il medesimo messaggio viene inviato identico a venti persone, o si può immaginare una parte del suo contenuto, gli analisti dispongono di una base di lavoro molto più ricca; alcuni affermano che si possano ricavare dati utili misurando il tempo che i computers impiegano per le operazioni di cifratura. E' quindi certo che anche di fronte ai migliori metodi di criptazione i laboratori della CIA o dell'FBI possono tentare qualcosa (*cosa* è ovviamente un segreto ben custodito), ma occorre essere realisti: se un'organizzazione così potente è davvero interessata a violare la chiave crittografica di qualcuno, troverà in genere assai più semplice ed economico accedere fisicamente al computer dell'interessato e prelevare in chiaro ciò che desidera, oppure corrompere un collaboratore, o persino intercettare da un ambiente vicino gli impulsi elettromagnetici emessi dalla tastiera: avvalersi, insomma, delle "normali" tecniche di spionaggio industriale.

<sup>5</sup> Il Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Gazzetta Ufficiale n. 60 del 13 marzo 1998) all'articolo 9 vieta alle Autorità di Certificazione di ricevere chiavi private, che ai sensi dell'articolo 7 del medesimo DPR possono essere depositate con le forme del testamento segreto.

<sup>6</sup> 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. Può ipotizzarsene, senza cadere nella fantascienza, anche un uso in campo contrattuale. Se ad esempio ho affittato per il mese d'agosto una villetta in Grecia di cui l'agenzia mi ha inviato via Internet un video, è una buona idea allegare il video al contratto di locazione, ed apporre al tutto la firma digitale. Qualora l'agenzia tentasse di affibbiarmi una casa diversa ...

<sup>7</sup> Questa è 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 IQMFE DL3Wb ofdJ 5Z XcaOyQEB AWw EAJH5 YQu3Y/ozsN». Che poi il testo alternativo, oltre a significare qualcosa, possa tornare in concreto utile all'eventuale manipolatore, è ipotesi del tutto inverosimile.

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. Questo spiega perché un messaggio provvisto di firma digitale possa essere trasmesso anche attraverso reti intrinsecamente insicure (come Internet)<sup>9</sup>, 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.

Nulla vieta, naturalmente, di eseguire entrambe le operazioni sul medesimo messaggio, che sarà quindi firmato digitalmente e leggibile solo dal destinatario<sup>10</sup>.

I moderni softwares di posta elettronica fanno sì che la verifica della firma avvenga senza che l'utente debba preoccuparsi di premere neppure un tasto: il programma, constatata l'esistenza di una firma digitale su un messaggio in arrivo, si collega automaticamente con l'archivio delle chiavi pubbliche, verifica la firma, e fa apparire sul video un'icona: firma verificata (o non verificata, se del caso). L'operazione di firma o di criptazione è appena più complicata. La chiave segreta è contenuta sulla *smart card*, che ha le dimensioni di una carta di credito: questo sia per evitare di lasciare un dato così delicato all'interno di un computer, sia per consentirne l'uso (itinerante, per così dire) con qualunque computer attrezzato all'uopo. Si sceglie il file da firmare, si introduce il proprio PIN (come nel Bancomat), si clicca su "Firma" e l'operazione è conclusa.

Vi è in quanto fin qui descritto un evidente punto debole: come può il destinatario del messaggio essere certo che la chiave pubblica che egli adopera per la verifica appartenga veramente al mittente? Sotto un diverso angolo visuale: come può il destinatario dimostrare la riferibilità della

---

<sup>8</sup> 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; ma se l'immagine biometrica venisse usata 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 sul PIN (Personal Identification Number), come il Bancomat. Si veda però *infra*.

<sup>9</sup> Un sistema a chiavi simmetriche richiede invece l'uso preventivo di un canale di comunicazione sicuro: ad esempio, la fisica consegna al comandante di un sommergibile, prima della partenza, del codice in plico sigillato. I sistemi simmetrici sono però di funzionamento molto più rapido, e si è quindi pensato ad utilizzare inizialmente una connessione a chiavi asimmetriche come canale sicuro per comunicare segretamente una chiave simmetrica, da usarsi poi durante il resto della comunicazione. La tecnica è molto vantaggiosa quando debbano scambiarsi una gran quantità di dati criptati, ad esempio durante le operazioni di shopping *online*. Il sistema SSL, sviluppato da Netscape, funziona ad esempio nel modo seguente. Il server con cui ci si sta collegando comunica la propria chiave pubblica al computer del utente; il software si occupa di verificare presso una *Certification Authority* (su cui *infra* nel testo) 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 punto condividono segretamente una loro esclusiva chiave simmetrica, possono utilizzarla per la successiva comunicazione. Questa procedura, oltre a consentire una maggior velocità, 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.

<sup>10</sup> Non si tratta di una semplice esercitazione tecnica: 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.

chiave al mittente onde contrastare un eventuale tentativo da parte di quest'ultimo di disconoscere il documento od il suo contenuto?

Entra qui in campo la cosiddetta *Certification Authority*, ente pubblico o società provvista di requisiti analoghi a quelli richiesti per l'esercizio dell'attività bancaria. La sua funzione<sup>11</sup> è attestare a chi appartenga una determinata chiave pubblica: all'uopo deve procedere innanzitutto alla materiale identificazione dell'interessato, mantenendo le informazioni a disposizione di chiunque in un archivio *online*, da cui far emergere anche l'eventuale cessazione di validità della chiave, per avvenuta scadenza o revoca. Sulla base delle risultanze dell'archivio chiunque può dimostrare che un determinato documento è stato firmato con la chiave, valida e non scaduta, di Tizio (od almeno: della persona che la *Certification Authority* ha identificato come Tizio).

Il sistema pone evidentemente delicatissimi problemi di responsabilità, connessi all'accuratezza dell'identificazione ed all'efficiente (e tempestiva!) gestione dell'archivio. Ancora non del tutto risolti sono inoltre alcuni problemi legati alle speciali attribuzioni di firma che possono competere ad un determinato soggetto<sup>12</sup>. L'analisi di tale problematica va ben al di là delle possibilità di questo brevissimo scritto; si consentirà pertanto di prescindere, assumendo quale ipotesi di lavoro che i malfunzionamenti del sistema siano assolutamente trascurabili.

Resta un ulteriore passaggio: il fatto che la chiave pubblica appartenga a Tizio, non vuol dire che una determinata firma digitale sia stata apposta da Tizio. Può darsi che egli abbia affidato la propria *smart card* a qualcun altro, rivelandogli anche il relativo PIN; la firma così apposta è totalmente indistinguibile da quella realizzata direttamente dal titolare. Se Tizio è un imprenditore, possiamo metabolizzare una simile eventualità riconducendo i rischi di abusivo utilizzo della firma

---

<sup>11</sup> Il citato Decreto del Presidente della Repubblica 10 novembre 1997, n. 513, articolo 9 stabilisce, al secondo comma, che il *certificatore è tenuto a:*

*identificare con certezza la persona che fa richiesta della certificazione;*

*rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 3;*

*specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;*

*attenersi alle regole tecniche di cui all'articolo 3;*

*informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;*

*attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;*

*non rendersi depositario di chiavi private;*

*procedere tempestivamente alla revoca od alla sospensione del certificato 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;*

*dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche;*

*dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.*

<sup>12</sup> Il dottor Romolo Romani possiede come privato cittadino una coppia di chiavi, e con questa è libero di concludere tutti i contratti telematici che desidera. Ma quando egli viene nominato notaio in Roma, deve in qualche modo risultare questa sua qualifica, in forza della quale le copie autentiche di atti e le realtive note di trascrizione digitalmente firmate debbono essere accettate da qualunque Ufficio del Territorio d'Italia (e, tendenzialmente, d'Europa). Chi è abilitato ad ordinare la pubblicizzazione di questa qualifica? Il Presidente del Consiglio Notarile, evidentemente: il Presidente deve essere dunque provvisto di una chiave (o di più chiavi) con triplice valenza: privato cittadino, notaio e Presidente. Può capitare poi che il giorno dell'iscrizione a ruolo di Romolo Romani il Presidente sia assente; provvederà il Consigliere Anziano. Anche quest'ultimo dovrà quindi possedere una triplice capacità di firma digitale, con l'ulteriore complicazione che i suoi poteri di firma quale Consigliere Anziano dovranno essere condizionati all'assenza del Presidente.

all'area del più generale rischio d'impresa; nel caso di un privato le cose si fanno evidentemente più delicate, almeno da un punto di vista sociale.

La tecnologia si propone di risolvere anche questo problema. La *smart card* può incorporare alcuni dati biometrici del soggetto: l'impronta digitale, la forma della mano o del viso, la voce, l'immagine della retina o dell'iride. Il sistema può quindi essere impostato in modo da impedire l'apposizione della firma laddove il titolare non dimostri di essere presente appoggiando le dita su un lettore d'impronte digitali od avvicinando l'occhio ad una telecamera. Tali sistemi, già entrati nell'uso comune<sup>13</sup>, pongono peraltro significativi problemi di sicurezza<sup>14</sup>.

A rigore, non si può quindi affermare che la firma digitale assicuri in modo assoluto l'identificazione del sottoscrittore; per converso è del tutto ragionevole immaginare che nel complesso i rischi siano assolutamente accettabili, e non superiori a quelli connessi all'impiego di sistemi cartacei.

Occorre a questo punto porsi con franchezza una domanda. Quale significato può conservare, in un simile contesto, il ruolo del notaio?

Un dato deve essere messo a fuoco con assoluta chiarezza. L'identificazione delle parti è un passaggio ineliminabile ma ormai di secondaria importanza nell'ambito della funzione notarile. Il baricentro dell'attività notarile sta da tempo altrove: nell'attività di informazione e di assistenza dei contraenti, sul piano civilistico come su quello fiscale; nella ricerca delle soluzioni che meglio realizzano le intenzioni delle parti. La particolare autorevolezza del notaio, che gli deriva sia dalla

---

<sup>13</sup> Gli sportelli ATM (l'equivalente dei nostri Bancomat) della Royal Bank of Canada e della Canadian Imperial Bank of Commerce in Toronto utilizzano come riconoscimento l'immagine dell'iride dei clienti; la geometria della mano è stata utilizzata per l'identificazione degli atleti alle Olimpiadi del 1996.

<sup>14</sup> Nessuna tra le tecnologie descritte è infatti in grado di assicurare una identificazione totalmente sicura, e sfortunatamente i sistemi migliori (quelli basati sulla struttura della retina) impongono all'utente di sottoporsi ogni volta all'illuminazione ed ispezione dell'interno dell'occhio da parte di una telecamera, il che risulta sgradito a molti; se simili considerazioni sono poco rilevanti in ambito militare, oppure nella gestione dell'accesso alla sala di controllo di una centrale nucleare, divengono vitali per sistemi da proporre alla generalità del pubblico. Per converso le tecnologie meno intrusive (identificazione della voce o della struttura facciale) sono anche le meno sicure: per ingannare due diversi sistemi di riconoscimento del viso è stato sufficiente applicarsi sul volto a mo' di maschera una foto della persona conosciuta dal sistema, praticando un foro all'altezza del naso per garantire un minimo di tridimensionalità; (il test è stato eseguito dalla redazione della rivista americana *PC Magazine*, ed è apparso sul numero del 23 febbraio 1999: <http://www.zdnet.com/pcmag/features/biometrics/break.html>). Per rendere più sicuri tali strumenti occorre impostare parametri operativi particolarmente stringenti, con l'effetto però di aumentare a dismisura gli errori in senso inverso, e cioè i dinieghi di identificazione del vero titolare, che sono fastidiosissimi per l'utente. I sistemi basati sull'impronta digitale appaiono in definitiva un compromesso ragionevole, anche perché il loro costo è ormai del tutto accettabile, sotto la soglia psicologica dei 100 dollari anche per prodotti di gran marca. La sicurezza è pure molto buona: Sean Connery / James Bond in *Diamonds Are Forever* (1971; in italiano *Agente 007, Una cascata di diamanti*) applicava sui polpastrelli una pellicola trasparente che recava incise le impronte digitali di qualcun altro, ma nella realtà pare non funzioni. Ed è probabilmente solo ironia quella del celebre sito americano <http://www.salon.com> quando propone la specialità medica *Biometric forgery* (falsificazione biometrica) come una delle professioni emergenti del 2002 <http://www.salon.com/21st/feature/1998/01/05feature.html>. I sistemi possono però essere violati ad un livello puramente informatico. 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: ma un'impronta digitale? A questo si tenta di rimediare con tecnologie complesse, in cui il dato biometrico viene utilizzato come componente di un più elaborato algoritmo crittografico, cosicché i dati scambiati tra gli apparati coinvolti nel procedimento di identificazione varino ad ogni sessione. Infine un dettaglio un po' raccapricciante: la retina decade pochi minuti dopo la cessazione del flusso sanguigno, per cui l'asportazione dell'occhio a fini di pirateria biometrica parrebbe fortunatamente improbabile. Per le dita, invece ...

sua specifica ed approfondita preparazione, sia dall'essere Pubblico Ufficiale al di sopra delle parti (e non al servizio di una parte), fa sì che la stragrande maggioranza delle operazioni possa essere conclusa col suo solo intervento, senza cioè che ciascuna delle parti debba sobbarcarsi il costo di un proprio consulente. Molte controversie vengono anche bonariamente composte con l'aiuto del notaio, prima che sfocino in vere e proprie cause. Il notaio svolge inoltre una funzione di pubblico interesse. In primo luogo limita, attraverso la sua opera preventiva<sup>15</sup>, l'intasamento della giustizia: in Europa, ove con pochissime eccezioni operano notariati organizzati in modo molto simile a quello italiano, le controversie nelle materie di competenza notarile sono enormemente meno numerose rispetto a quanto accade, ad esempio, negli Stati Uniti, con costi globalmente molto inferiori per la collettività. Sviate norme di legge assegnano infine al notaio, oltre al tradizionale controllo di legalità degli atti, specifiche funzioni nell'ambito della repressione dell'abusivismo edilizio, dell'evasione fiscale, del riciclaggio di denaro sporco in attività economiche.

L'insieme di queste funzioni non rappresenta in alcun modo un retaggio del passato: la maggior parte dei compiti appena citati derivano anzi da legislazione recente, dell'ultimo quindicennio<sup>16</sup>. Tale trend ha riscontro a livello mondiale: il notariato come noi lo conosciamo in Italia, il cosiddetto notariato latino, sta vivendo una fase di grande diffusione: al tradizionale nucleo storico (tra cui Italia, Francia, Germania e Spagna) si sono affiancate numerosissime altre realtà, a cominciare dal Giappone; i Paesi che nell'ultimo decennio si sono affacciati all'economia di mercato, soprattutto nell'Est Europeo, hanno aderito in massa al modello latino, ivi compresa la stessa Russia. Oltre settanta Paesi<sup>17</sup> sono oggi dotati di un'organizzazione notarile di tipo latino.

Non solo la firma digitale non potrà quindi sostituire la funzione notarile<sup>18</sup>: è anzi probabilmente vero il contrario. Per averne riscontro, basta guardare a ciò che sta avvenendo negli Stati Uniti.

Il Public Notary americano è una figura di assai ridotta qualificazione professionale, il cui compito si limita all'identificazione del sottoscrittore<sup>19</sup>. Ne discende, tra l'altro, che i documenti notarili americani sono accettati con difficoltà al di fuori degli Stati Uniti; ciò è già sufficientemente grave in un sistema basato su documenti cartacei, ma rischia di divenire esiziale nel mondo telematico, globale per definizione. Una parte significativa del mondo giuridico statunitense guarda quindi da tempo all'istituzionalizzazione del sistema di firme elettroniche come ad una felice

<sup>15</sup> L'approccio di tipo preventivo si va diffondendo anche negli USA, stimolato dal mostruoso ammontare delle spese per attività contenzione in quel Paese: si veda il sito Internet <http://www.preventive-law.org>

<sup>16</sup> Legge 28 febbraio 1985 n. 47; decreto legge 27 aprile 1990 n. 90 (convertito con legge 26 giugno 1990 n. 165); legge 12 agosto 1993 n. 310.

<sup>17</sup> Riuniti nell'Unione Internazionale del Notariato Latino (UINL) che la stessa Verisign, società statunitense leader nel campo della firma digitale, definisce *the world's most influential and prestigious notarial organization* (<http://www.verisign.com/repository/notryfaq.html>). Il sito web dell'UINL è all'indirizzo <http://www.onpi.org.ar>

<sup>18</sup> In tal senso l'attuale normativa italiana: articoli 4, 5 e 16 del DPR 513, *cit.*

<sup>19</sup> Visto che tutto è circoscritto all'identificazione, sembrerebbe naturale che in USA le firme digitali siano equiparate a quelle autenticate dal Public Notary; e così in effetti è in alcune legislazioni, ad esempio quella dello Utah. Cionondimeno, è interessante notare che alcuni studiosi americani avversano anche questa assimilazione. C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 *San Diego Law Review* 1143, 1996 (su Internet alla pagina <http://www.acusd.edu/~biddle/mp.html>) osserva che la sottoscrizione dinanzi al Public Notary ha anche la funzione di richiamare l'attenzione dell'interessato intorno all'importanza dell'atto che sta per compiere (la terminologia americana è fulminante: *Ceremony*). Il titolare di una coppia di chiavi compare invece una sola volta dinanzi all'autorità certificante, in occasione della certificazione della chiave stessa, che è destinata ad essere usata per la firma di un numero illimitato di documenti. L'Autore giudica pertanto pericoloso che le firme digitali siano assimilate alle sottoscrizioni autenticate dal Public Notary.

occasione per colmare una lacuna del proprio sistema. In questo contesto emerge la proposta, fatta propria dall'American Bar Association <sup>20</sup>, di istituire negli USA una nuova figura professionale, denominata appunto *Cybernotary*, espressamente ispirata al notaro di tipo latino, cui affidare la produzione di documenti dotati di elevata credibilità sul piano internazionale <sup>21</sup>. Il primo Stato dell'Unione a dotarsene è stato, nel maggio 1997, la Florida <sup>22</sup>.

Con ciò si compie una duplice, incrociata nemesi storica: la miglior conferma della vitalità del modello latino proviene dall'area geografica che più flagrantemente ne aveva finora ignorato l'esistenza stessa, ed è maturata all'interno di un settore, quello dell'informatica e della telematica, che per mero pregiudizio viene talora inquadrato in termini di antagonismo od incompatibilità con il notariato stesso.

Nel frattempo, si sta per passare alla pratica. I notai italiani saranno certamente tra i primi ad avvalersi su larga scala della firma digitale, soprattutto nella trasmissione dei documenti tra loro e nei confronti della Pubblica Amministrazione. Anche degli atti originariamente creati in forma cartacea potranno essere prodotte copie in forma digitale <sup>23</sup>, da trasmettere ad esempio via Rete ai pubblici uffici in modo economico e veloce per le formalità di registrazione, iscrizione, trascrizione e volturazione, per la maggior sicurezza di tutti.

---

<sup>20</sup> La homepage del comitato dell'American Bar Association per l'istituzione del Cybernotary è <http://www.abanet.org/scitech/ec/cn/home.html>

<sup>21</sup>

Tra gli obiettivi del comitato di cui alla nota precedente rientra il riconoscimento degli atti del Cybernotary in ambito NAFTA. La dice lunga sull'arretratezza del notariato americano il fatto che da parte USA si debba porre in agenda il conseguimento dell'efficacia degli atti notarili a stelle e strisce in territorio messicano, mentre quelli italiani sono riconosciuti di diritto, senza alcuna previa formalità, in Francia, Germania, Danimarca... Ciò non dipende dall'appartenenza all'Unione Europea, ed infatti il Regno Unito (paese di *common law*, come gli USA) vive una situazione simile a quella americana, appena mitigata dall'esistenza di un apposito ristrettissimo corpo specializzato basato a Londra, i *Scrivener Notaries of the City of London*, per la redazione di atti notarili destinati ad essere utilizzati all'estero. I notai londinesi (e non la generalità dei notai inglesi, si badi bene) sono stati di recente ammessi a far parte dell'Unione Internazionale del Notariato Latino. L'evento è commentato sul sito Internet dello studio notarile John Venn & Sons con queste parole: *This is a significant event in the history of Notaries around the world, in that it is the first time that Notaries from a Common Law based legal system have been recognised as having the same status as their Civil Law colleagues* (è un evento significativo nella storia del notariato nel mondo, giacché è la prima volta che a notai provenienti da un paese di Common Law è riconosciuto il medesimo status dei loro colleghi del mondo del diritto civile): <http://www.cix.co.uk/~kennair/title.htm> La Corte di Giustizia Europea, da parte sua, ha recentemente ribadito l'insostituibilità della funzione notarile sancendo che un atto formato senza l'intervento del notaio non può in nessun caso essere equiparato ad un documento autentificato, neppure se il Paese dell'Unione in cui il documento è stato formato non prevede affatto il ministero notarile: sentenza nel procedimento C-260/97, Unibank A/S vs. Flemming G. Christensen, *Foro Italiano*, 1999, IV, c. 513, reperibile anche presso il sito <http://www.curia.eu.int/it/index.htm>

<sup>22</sup>

Act of May 30, 1997. Florida 1997 Statutes, chapter 118, section 10 (reperibile via Internet alla pagina <http://www.leg.state.fl.us/citizen/documents/statutes/1997/ch0118/e10%5F%5F%5F.htm>).

<sup>23</sup>