CONSIGLIO NAZIONALE DEL NOTARIATO

Commissione Informatica

Efficacia, rilevanza formale, rilevanza probatoria
Firme Elettroniche - Questioni ed esperienze di diritto privato, Milano, 2003

1. Il quadro normativo attuale è segnato in modo determinante dalla Direttiva europea 93/1999 **(1)** che, a differenza della previgente legislazione italiana, non contempla una figura unitaria e standardizzata di firma digitale, ma prevede una sorta di *continuum*, capace di accogliere un ventaglio indefinito di tipologie.

Al vertice la f*irma 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 figura che, secondo un uso consolidato, è detta in Italia *firma digitale* **(2)**. 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.*

In quest'ultima categoria possono rientrare figure assai varie per sicurezza ed affidabilità: persino un *cookie* **(3)** od un messaggio SMS paiono astrattamente riconducibili alla definizione della Direttiva. Coerentemente, il legislatore comunitario ha però differenziato lo *status* delle due figure sotto il profilo probatorio, con un approccio (art. 5) 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 di per sé speciali problemi; le difficoltà, come si vedrà più innanzi (§ 2.3) derivano piuttosto dal criterio seguito in sede di attuazione nel nostro Paese.

Per le firme elettroniche minori (dette anche semplici, o leggere) la Direttiva stabilisce che: *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.*

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,.

2. La scelta di attribuire valore giuridico alle firme elettroniche minori corrisponde ad un'esigenza riscontrata nell'evoluzione del commercio elettronico.

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 cosiddetto *e-commerce*. Tale prognosi non ha trovato conferma nell'esperienza pratica degli anni recenti, né in Italia né a livello internazionale.

Vi è consenso sulle ragioni di tale fenomeno **(4)**. Gli operatori del settore hanno a propria disposizione strumenti informatici assai più semplici **(5)**, che non pongono a carico dell'utente una fastidiosa fase di registrazione e certificazione **(6)**. 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 **(7)**. 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 alquanto contenuto, ed il numero di esse è notevolmente alto. Anche laddove un certo numero di esse non abbia buon esito, 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 ad elevatissima sicurezza ma cui pochi consumatori accederebbero a causa delle inevitabili complicazioni.

Il legislatore comunitario ha dunque compiuto una scelta appropriata quando, come s'è visto, ha attributo rilevanza alla firma elettronica semplice, operando "in negativo", impedendo cioè che gli ordinamenti nazionali ne disconoscano *tout court* l'efficacia. Scelta compiuta in piena consapevolezza, come risulta dai *considerando* che precedono l'articolato, e che esprimono l'obiettivo di promuovere lo sviluppo delle nuove tecnologie in generale e delle firme elettroniche in particolare, garantendo una sia pur limitata tutela a qualunque strumento di autenticazione dell'autore del documento informatico. Va poi considerata, nell'apprezzare la tecnica della Direttiva, la costante necessità di far convivere i due diversi sistemi giuridici presenti in ambito comunitario: quello di *common law* basato sulla valutazione del giudice anche in assenza di precetto, e quello di *civil law* che in linea di principio non ammette tale ipotesi.

In sede di attuazione della direttiva il legislatore delegato italiano si è però spinto molto più innanzi, senza che la direttiva lo richiedesse. L'art. 6 comma 2 del D.Lgs 10/2002 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. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare".

La firma elettronica leggera 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 **(8)**: una firma elettronica semplice potrà essere utilizzata per sottoscrivere (validamente!) 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 **(9)**, 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 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 **(10)**.

Di tutto questo pare in qualche modo cosciente il legislatore nazionale 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* **(11)**, 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 (12), ma è anche (e forse: soprattutto) predisposizione del mezzo di prova **(13)**. 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, nella cui prassi si ricercherebbero invano fattispecie riconducibili all'alveo dell'articolo 1350 cc, fornisca un astratto quanto inutile *status* di forma scritta, e nessuna certezza sul piano probatorio.

Non minori perplessità desta il rinvio che il Decreto opera all'articolo 2214cc: le scritture contabili possono essere regolarmente tenute avvalendosi di qualunque tipo di firma elettronica. Fatto è che le scritture contabili hanno funzione probatoria (articoli 2709 ss): resta alquanto misterioso come possano all'uopo essere state reputate idonee le firme elettroniche "minori", che la medesima legge (anzi: il medesimo comma) riconosce esser poco attendibili proprio sul piano probatorio **(14)**.

3. La disposizione della legge d'attuazione che ha attirato le più serrate perplessità è senza dubbio quella di cui all'articolo 6 comma 3: Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto. La prima ed ovvia reazione è stata individuare nella norma un'indebita equiparazione della firma digitale alla scrittura autenticata. Equiparazione formale che peraltro tutto è fuorché una novità, dato che era stata intravista dalla dottrina più attenta **(15)** già nell'imperio della previgente normativa. Questo non è però che l'inizio del problema.

Prendiamo a riferimento, in luogo della scrittura autenticata, il regime della scrittura privata semplice, come risultante dal combinato disposto dell'articolo 2702 cc e degli articoli 214 e 215 cpc. In cosa differisce la nuova norma? Non nell'efficacia probatoria sino a querela di falso, che c'era già, quanto nella caduta del meccanismo del riconoscimento. Ma è concepibile un sistema di riconoscimento applicato alla firma digitale?

Una firma digitale non può dirsi neppure una firma (è solo una sequenza informe di *bytes*) se non è verificata sul piano informatico **(16)**, se cioè non si accerta che la firma apposta è compatibile con la chiave pubblica del sottoscrivente **(17)**. Compiuto con esito positivo tale *test,* si ha la ragionevole certezza che quella determinata firma è stata apposta utilizzando un determinato dispositivo di firma (*smart card* od altro supporto idoneo **(18)**. Ragionevole certezza, e nulla più: anche da un 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 mera difficoltà di calcolo. La

falsificazione della firma digitale (o meglio, la rivelazione del segreto di chiave) è quindi eventualità non del tutto da escludersi, soprattutto se si considera che eventuali falsificatori hanno a propria disposizione strumenti assai più efficaci del cosiddetto *brutal attack* **(19)**.

Non solo: il dispositivo di firma può essere stato utilizzato da chiunque abbia ottenuto (col consenso del titolare, o con l'inganno o la violenza) il relativo PIN. A differenza di una perizia calligrafica, il *test* nulla ci dice quindi su chi abbia realmente manovrato il dispositivo; detto in altri termini, sappiamo che la firma viene da quella *smart card*, ma non che sia stato davvero Tizio a firmare **(20)**. Per questa ragione diversi studiosi **(21)** giustamente reputavano più corretta la definizione di sigillo, anziché firma, digitale. L'equivoco continua a mietere vittime, dato che anche la normativa più recente discorre di "chi ha sottoscritto" un documento: soggetto la cui identità, a ben riflettere, resta perfettamente ignota.

Se trasportiamo queste ovvie considerazioni sul piano probatorio, la nebbia si fa fitta **(22)**. Non si può certo pretendere che chi intende valersi della firma provi che il congegno è stato davvero manovrato da Tizio: salvo casi eccezionalissimi, come potrebbe? Equivarrebbe in pratica ad azzerare il valore giuridico della firma digitale. Ogni altra strada conduce a far gravare su Tizio, su base oggettiva, il rischio di ogni uso improprio della *smart card* da lui fatta emettere.

Anche laddove si riconoscessero a Tizio margini di prova contraria, questi risulterebbero infatti di interesse poco più che scolastico: neppure Tizio potrebbe verosimilmente dimostrare di non essere stato lui. Non si pensi alle ipotesi di smarrimento e sottrazione del dispositivo di firma, che 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 **(23)**.

Sotto questo limitato angolo visuale l'opzione del legislatore delegato, per quanto criticabile, appare a prima vista, se non altro, meno insensata: si spazza via un meccanismo che avrebbe avuto scarsa possibilità d'applicazione pratica. In quest'ottica, non appare irragionevole che si lasci a disposizione del titolare solo l'*extrema ratio* della querela di falso **(24)**. Il problema è che in tal modo non si disinnesca la potenziale pericolosità del sistema: ci si limita a stabilire chi debba correrne i rischi **(25)**.

Vi sono però altre fattispecie tutt'altro che teoriche che, per usare un eufemismo, pongono a dura prova il concetto di "piena prova sino a querela di falso". La più evidente è 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 **(26)**. 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 **(27)** da parte del defunto equivalga al conferimento di una forma peculiare di potere rappresentativo: in tale prospettiva potrebbe

reputarsi applicabile l'articolo 1396 c.c., secondo comma, così salvaguardando la buona fede del terzo. Ad analogo esito si può forse pervenire facendo applicazione del principio dell'apparenza imputabile **(28)**.

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.

Che il disconoscimento non continui ad essere uno strumento degno di considerazione anche con riferimento alla firma elettronica resta in sostanza da dimostrare. Pare anzi auspicabile che l'ordinamento definisca in quali circostanze, con quali modalità e a carico di chi sia possibile dimostrare che una firma elettronica sia stata manomessa, contraffatta, o utilizzata illegittimamente, definendo le responsabilità dei soggetti coinvolti (titolare del certificato di firma **(29)**, certificatore, terzo destinatario del documento firmato).

Il problema più serio è però, come suol dirsi, a monte: il ruolo esagerato che il sistema finisce con l'attribuire ai certificatori. La sicura attribuibilità di una firma ad un determinato soggetto evidentemente dipende, in radice, dall'accuratezza dell'identificazione compiuta in sede di rilascio del certificato. L'osservazione è banalissima, ma cionondimeno (o forse proprio per questo) stranamente trascurata **(30)**: 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. L'efficacia probatoria privilegiata sancita dalla nuova norma, avendo ad oggetto, *omisso medio*, l'associazione tra il titolare e la firma, copre per necessità logica ciascuna delle due fasi. Anche tralasciando 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 **(31)**. Ed ogni catena, per definizione, non può essere più solida del più debole dei suoi anelli **(32)**.

Tale funzione viene svolta in proprio dai certificatori oppure delegata dai certificatori alle Registration Authorities, soggetti esterni: società di servizi **(33)** ed agenzie di disbrigo pratiche, ad esempio, che agiscono tramite propri dipendenti. Istruttivi casi di falsificazione ai massimi livelli **(34)** si rinvengono già nell'esperienza internazionale.

La norma introdotta dal legislatore delegato **(35)** finisce dunque con l'equiparare indirettamente questi soggetti ai pubblici ufficiali, atteso che l'unico strumento a disposizione resta la querela di falso. E questo pare davvero troppo **(36)**. Non si intende neppure entrare nella ben nota querelle su quale *standard* di accuratezza sia imposto al certificatore **(37)**. L'obiezione è più radicale: non si vede perché il titolare apparente del certificato debba

obbligatoriamente far ricorso alla querela di falso per porre in discussione l'operato di un semplice soggetto privato, la cui attività (ai sensi dell'articolo 3 della direttiva, attuato con l'articolo 3 del D.Lgs. 10/2002) non è neppure sottoposta a previa autorizzazione od iscrizione ad un albo, ma a semplice "avviso".

E non è tutto. Chi desideri vedere autenticata la propria firma da un pubblico ufficiale, deve dinanzi a lui comparire in occasione della sottoscrizione di ciascun documento. Il rilascio del dispositivo di firma digitale pare avere, nel corrente sistema, una valenza addirittura superiore, giacché attribuisce uno *status* giuridico privilegiato a tutta l'indefinita serie di documenti che con in base a quel certificato saranno firmati **(38)**.

Da ultimo: resta da stabilire se il gesto che dà vita alla firma digitale possegga davvero quel grado di riconoscibilità sociale che consenta all'ordinamento di attribuirle, senza traumi e disarmonie, le conseguenze giuridiche proprie della firma autografa. Non può certo trascurarsi ad esempio l'ipotesi che, per scarsa dimestichezza col mezzo, si attivi la procedura di firma in modo del tutto inconsapevole o che, per scarsa cultura informatica, si commettano grossolane imprudenze sul fronte sicurezza **(39)**. Si può anche ipotizzare che il sistema informatico dell'utente venga manipolato da intrusi, così che vengano firmati documenti che l'interessato non ha mai veduto. E nulla distingue tali sottoscrizioni da quelle scientemente apposte dall'utente **(40)**.

4. Si vede qui, meglio che in altri contesti, come una parte significativa della dottrina italiana trascuri quasi totalmente il peso dell'elemento umano e dei punti deboli di origine non informatica che si riscontrano nel sistema. Colpisce in particolare come ciò si ravvisi in massimo grado proprio tra gli autori che dimostrano meno dimestichezza col dato tecnologico, e dai quali sarebbe lecito attendersi una maggiore attenzione ai riflessi dell'agire degli operatori umani. Il fenomeno non è però inspiegabile. I giuristi che non spingono la propria analisi sino ad una revisione critica dell'iter tecnologico della firma, non hanno altra scelta che assumere passivamente all'interno della propria ricostruzione dati e valutazioni d'origine ed impianto culturale esclusivamente tecnico, la cui esatta natura può non coincidere affatto con quella che il giurista si attende. Affermazioni ineccepibili in un contesto tecnico, si trasformano in clamorosi errori laddove passivamente trasposte in un contesto giuridico.

E' ad esempio tecnicamente esatto affermare che ogni *file* (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. Un problema è appunto qui. L'espressione tecnico informatica "copia di un *file*" indica un'operazione che dal punto di vista concettuale è ben diversa dalla 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 una lunga sequenza di *bit,* o se vogliamo di lettere e numeri. Pretendere di distinguere originale e copia di un *file* equivale ad accusare un notaro di non aver indicato in atto il vero codice fiscale di una parte, ma solo una sua copia esatta. Questo conduce a forti perplessità intorno alla realizzabilità di cambiali, assegni, procure per un solo atto o copie in forma esecutiva in forma digitale: anche il documento firmato digitalmente (che, come si è detto, è solo un *file* come un altro) è duplicabile all'infinito senza alcuna variazione. Ed ovviamente non è pensabile (ad esempio) una cambiale digitale riproducibile in infiniti esemplari, tutti a pari titolo "originali" **(41)**. Ne discende che l'ineccepibile affermazione tecnica da cui si è partiti (ogni *file* è suscettibile di firma digitale) diviene a dir poco fuorviante se trasfusa in un contesto giuridico.

Infortuni di tal fatta sono inevitabili per il giurista che scelga di 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 **(42)**. Affidarsi alla passiva riproduzione di mal metabolizzate nozioni tecniche non è in alcun modo una soluzione: l'esito, paradossale 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.

5. Ipotesi di particolare interesse è quella dell'uso del dispositivo di firma digitale da parte di persona diversa dal titolare, ma col consenso di quest'ultimo.

Su un punto 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 l'affidamento a terzi della *smart card* da parte di un pubblico ufficiale **(43)**, e neppure da parte dell'amministratore di una società per adempimenti di sua inderogabile personale responsabilità.

Si afferma poi comunemente che il terzo deve trovare tutela a preferenza del titolare che avendo trasferito il possesso della chiave ad altro soggetto autorizzandone (o tollerandone) così l'uso, ha dato luogo all'apparente situazione per cui le dichiarazioni provenienti dal materiale utilizzatore del dispositivo appaiono all'esterno come se fossero genuinamente provenienti dallo stesso titolare. E lo stesso può affermarsi per il caso di insufficiente custodia del dispositivo di firma. L'affermazione deve in linea generale senz'altro approvarsi, anche se può probabilmente essere ammorbidita in relazione al disposto della già ricordata Direttiva 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 28 *bis* del DPR445/2000, aggiunto dal DLgs 10/2002. 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. Va appena ricordato come il Manuale Operativo relativo ai servizi di certificazione del Consiglio Nazionale del Notariato precisi a tal riguardo 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.

Secondo l'opinione prevalente il fenomeno del consapevole affidamento a terzo del dispositivo di firma (e del PIN od altra chiave d'accesso) è riconducibile al regime della rappresentanza **(44)**, talora in via diretta **(45)**, talaltra in via di applicazione analogica **(46)**.

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 rovesciamento di prospettiva. La *contemplatio domini*, nella logica dell'articolo 1388cc (e, in modo più 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 soggetto agente, ma il terzo rappresentato **(47)**. Se questo è esatto, rimarcare l'inesistenza della *contemplatio domini n*on 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.

Si può poi osservare che, ragionando in termini di rappresentanza, sopravviene la difficoltà di dar conto del rispetto del principio di cui all'articolo 1392cc. A tale osservazione si può replicare nel senso che qui si ha (almeno secondo gli autori che aderiscono a tale orientamento) un peculiare tipo di rappresentanza: l'imputabilità dell'atto al soggetto rappresentato non discende da un positivo conferimento di un potere, ma dall'aver dato origine ad una situazione, per dirla col Bianca **(48)**, di apparenza imputabile; tale ricostruzione sfugge dunque all'indicato principio. D'altra parte, il sistema non ignora casi in cui si ha equiparazione alla scrittura privata, almeno sul piano probatorio, in assenza sia dell'autografia che di procura scritta: si prenda l'esempio del telegramma "fatto consegnare" ai sensi dell'articolo 2705cc, primo comma.

La posizione più severa **(49)** 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, trovando sostegno nel dominate orientamento giurisprudenziale che qualifica in tal modo anche il cosiddetto falso consentito **(50)**.

Quest'approccio pecca probabilmente di eccessiva rigidità. Come è stato affermato, 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 **(51)**.

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 il marchiano errore concettuale di confondere il fatto in sé con la pratica 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.

Anche l'argomento desumibile dall'orientamento giurisprudenziale in tema di falso consentito deve forse essere stemperato alla luce di quella diffusa dottrina che ne ripudia l'eccessiva rigidità in favore di soluzioni meno apodittiche, graduate proprio in relazione alla natura del documento sottoscritto; si perviene ad affermare che l'autografia della firma non è normalmente requisito indefettibile per la sua qualità giuridica **(52)**. L'affermazione della liceità del falso consentito in scrittura privata è alquanto diffusa in dottrina **(53)**; secondo un'opinione relativamente recente **(54)** in caso di falso in scrittura privata, perché si integrino gli estremi della fattispecie delittuosa è assolutamente necessario che sussista una lesione concreta degli interessi di qualche altro consociato.

Allo stato, un'ulteriore obiezione, di natura sistematica, viene frapposta alla sanzione di falso. Questa deriva infatti dall'equiparazione al documento scritto, che per espressa previsione normativa interessa però anche la firma elettronica semplice: ad esempio, la tessera Bancomat. Discorrere di falso in relazione all'affidamento a terzi della tessera per un'operazione bancaria non è, in tutta evidenza, neppure proponibile **(55)**. Non pare agevole sottrarsi a tale impasse. Trarre argomento dal diverso *status* probatorio della firma digitale da quella elettronica semplice, significa compiere *ex* professo la scorrettezza metodologica di cui viene accusata l'opposta opinione, e cioè confondere gli aspetti sostanziali con quelli probatori. Negare la natura negoziale delle operazioni poste in essere con la firma elettronica semplice significa davvero negare l'evidenza, dacché le firme elettroniche semplici sono correntemente e quotidianamente utilizzate per compravendite o per ordinare bonifici. Resta poi da intendere quale risultato si conseguirebbe per tale via, atteso che il concetto di falso è riferibile al documento, non al negozio.

Occorre ancora domandarsi quale regime sia applicabile laddove il terzo sia al corrente dell'uso del dispositivo di firma da parte di soggetto diverso dal titolare. Appare qui congruo **(56)** affidarsi alle conclusioni correnti in materia di riempimento abusivo del biancosegno. Su tali basi si può concludere per l'annullabilità del contratto in virtù delle norme sull'errore ostativo laddove il soggetto diverso dal titolare faccia del dispositivo un uso indebito (e quindi *contra pacta*, ma non *absque pactis*), riconosciuto come tale da parte del terzo, o riconoscibile *ex* 1431cc. Se quindi, a titolo d'esempio, il terzo fosse conscio del fatto che un dispositivo di firma è stato affidato da un imprenditore ad altro soggetto per l'esecuzione di alcuni adempimenti formali, sarebbe certamente non meritevole di tutela l'affidamento da lui

eventualmente riposto in documenti a carattere negoziale sottoscritti con la medesima *smart card*. Laddove la prassi della consegna ad altro soggetto diventasse particolarmente diffusa e notoria per alcuni tipi di dispositivo ed in determinati contesti, potrebbe quindi persino derivarne, in modo strisciante, una generale sanzione de facto (potrebbe quasi dirsi: ambientale) di giuridica inaffidabilità dei documenti così sottoscritti.

6. Si è rilevato come il sistema disegnato dal legislatore italiano tenda ad attribuire alla firma digitale un grado particolarmente elevato di efficacia giuridica. Se ciò, come è nelle dichiarazioni formali (e non v'è motivo di dubitare della loro sincerità) deriva dal desiderio di contribuire alla diffusione dello strumento, è il caso di domandarsi se questa strategia sia destinata ad essere coronata da successo.

La risposta è fortemente dubitativa. Come già si è osservato, le soluzioni adottate dal legislatore non tendono a risolvere (né avrebbero potuto) i problemi della firma digitale, ma solo ad addebitare ogni costo e rischio all'utente finale. Ciò può trasformarsi in un boomerang, per un paio di ragioni almeno. In primo luogo lo strumento rischia di apparire al grande pubblico troppo pericoloso per essere davvero appetibile. In secondo luogo può indurre la giurisprudenza ad attenuare, con tecniche varie, la severità dei principi. Si immagini il caso dell'amministratore di una Società che consegni la *smart card* Infocamere ed il relativo PIN, per l'esecuzione di alcuni adempimenti, a Tizio, il quale lo impieghi invece per ordinare ad una Banca il trasferimento di tutte le risorse della Società su un proprio conto. *Stricto jure*, l'operazione è aggredibile con estrema difficoltà, ma riesce difficile immaginare un Giudice che non dia fondo a tutta la sua creatività giuridica nella ricerca di un qualche rimedio **(57)**. Ed è del tutto chiaro che la variabilità, l'incertezza e l'imprevedibilità di tali decisioni (almeno sino al consolidamento di orientamenti definiti) non possono che nuocere alla diffusione dello strumento **(58)**.

Ugo Bechini

_____

(1) Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (*Gazzetta Ufficiale delle Comunità europee* n. L 013 del 19 gennaio 2000 pagg. 12 - 20). Per una visione comparatistica delle legislazioni europea e d'Oltreatlantico, 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; sia però consentito rinviare alle critiche mosse all'Autrice in 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*, Giuffrè, Milano 2003) ove anche per una ricostruzione in prospettiva storica della legislazione italiana, e per la distinzione tra *Thick Laws* e *Thin Laws*.

(2) Le espressioni firma elettronica e firma digitale hanno un impiego ormai praticamente stabilizzato, che si ritrova pressocché 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. Vedasi anche retro, §1.

(3) I *cookies* sono piccole stringhe di dati che restano memorizzati in un *computer*, consultabili e modificabili dai siti con cui la macchina si collega; sono ampiamente utilizzati nel commercio elettronico, ad esempio per serbare traccia delle preferenze di un determinato cliente.

(4) Si veda l'acuta analisi di J.K. WINN, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, in *Idaho Law Review,* Volume 37, Issue 2 (2001) p. 353. 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 (ma meno sanguinose) considerazioni nella medesima direzione, G. ARNÒ e D. LISTA, *La firma digitale nell'ordinamento italiano e comunitario*, in *Rivista di Diritto Civile*, 2000, II, p. 781, p. 783; M. CAMMARATA ed E. MACCARONE, *Introduzione alla firma digitale,* cit. (7 / Serve anche al commercio elettronico?), in *Interlex* (*www.interlex.it*) 16/12/99; sia consentito aggiungere anche U. BECHINI, *Quando la smart card diventa un souvenir*, in *Interlex* (*www.interlex.it*), 21/9/01. C. M. 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) efficacemente scrivono: *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).

(5) 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 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. cit*., il travolgente successo del sistema SSL deriva dal fatto che non è una firma.

(6) 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*.

(7) Per una contrapposizione tra *Formalistic model* e *Risk-Based Model*, si veda W. FORD e M. S. BAUM, *Secure Electronic Commerce, Prentice Hall, Upper Saddle River* (New Jersey, USA) 2000, p. 67.

(8) 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

(9) Espressione tenuta a battesimo, a quanto ci consta, 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

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

(11) Si ripropone qui una formula presentata in U. BECHINI e M. MICCOLI, *La forma sine probatione* in *Notariato*, 2002, p. 329.

(12) 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.

(13) Qualche rapido *click* del mouse sembra ancor meno idoneo a soddisfare l'altra tradizionale funzione attribuita alla forma, la responsabilizzazione del contraente. Ben altro discorso, anche qui, per la firma digitale propriamente detta: gli attuali *softwares*, pur non presentando la benché minima difficoltà di carattere informatico, hanno un'articolazione che conferisce al gesto della sottoscrizione un più che rispettabile grado di solennità.

(14) E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, cit., p. 1139. F. SORRENTINO *(Nuova disciplina sulle firme elettroniche*, in *Le Nuove Leggi Civili Commentate*, p. 294) avanza una critica in qualche modo opposta, giudicando eccessivo imporre una firma elettronica quando le scritture contabili tenute su carta non richiedono alcuna sottoscrizione, sempre che vi siano altri elementi idonei ad attribuirne la provenienza all'imprenditore. Ma qui è il punto: la firma elettronica semplice non è una vera sottoscrizione, in quanto non assicura nulla più di un non meglio specificato legame tra il materiale elettronico ed il suo autore (o il soggetto cui il materiale stesso è imputabile). Sotto questo profilo, quindi, la soluzione legislativa realizzerebbe semmai un azzeccato parallelismo: il problema è che la firma elettronica semplice non offre protezione contro le manipolazioni successive delle scritture: neppure quella, pur minima, garantita dal più informale degli scritti.

(15) R. ZAGAMI, *Firma digitale e sicurezza giuridica,* CEDAM, Padova 2000, p. 182, già scriveva: … in sostanza l'efficacia probatoria del documento informatico con firma digitale diviene in realtà diversa e superiore rispetto all'efficacia probatoria della scrittura privata cartacea come delineata all'articolo 2702cc, avvicinandosi piuttosto alla scrittura privata autenticata ex art. 2703cc. Questione completamente diversa, naturalmente, è stabilire se

la firma elettronica o digitale rappresenti una minaccia alla funzione notarile, ipotesi brillantemente demolita da B. REYNIS, *Signature électronique et acte authentique: le devoir d'inventer* (relazione al XXII Congresso annuale del Comitato Francoitaliano del Notariato Ligure e Provenzale, Genova, settembre 2001, sul tema *Atti autentici in Europa e firma elettronica) http://web.tiscali.it/conoge/italofrancese/ge.htm.* Osserva REYNIS che la funzione del notaro è ben altro che l'identificazione della parti: è garanzia di legalità, assistenza alle parti per il perseguimento dei loro obiettivi.

(16) E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, cit., p. 1138, fanno osservare che si tratta di vera e propria assenza di sottoscrizione, non di firma apocrifa.

(17) Al più si può forse immaginare che una firma digitale inverificabile come tale possa integrare gli estremi di una firma elettronica leggera, in un fenomeno assimilabile alla conversione; ciò potrebbe condurre ad ipotizzare che non di inesistenza si tratti, ma di semplice nullità.

(18) S. TONDO (*Note sull'autenticazione di scrittura elettronica*, in *Foro Italiano*, 2002, V, 212, nota 17) dopo aver fatto trapelare un qualche disdegno ad entrare in argomento, prende in considerazione solo l'ipotesi di utilizzare all'uopo un *floppy disk*. Il suggerimento è ineccepibile dal punto di vista tecnico/informatico: la chiave privata è una sequenza di dati memorizzabile ovunque (anche su pietra, se lo si desidera), e ad esempio le chiavi PGP vengono in effetti comunemente memorizzate su *floppies*. Si tratta però di un marchiano errore sul piano civilistico, dato che una firma apposta valendosi di un siffatto dispositivo non risponde in alcun modo né alla normativa europea né alla legislazione interna. E non potrebbe essere altrimenti, visto che una chiave su floppy disk può essere asportata senza speciali difficoltà ed utilizzata da chiunque.

(19) 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. Nel mondo reale, però, le minacce sono più sofisticate, e fanno per lo più leva su sagaci accorgimenti che sfruttano errori di concezione dei *softwares*. Una vecchia edizione del sistema SSL venne ad esempio messa alla berlina nel 1996 da due studenti di Berkeley, I. GOLDBERG e D. WAGNER, che riscontrarono alcune falle decisamente ingenue; il loro lavoro, *Randomness and the Netscape Browser*, è accessibile alla pagina *http://www.ddj.com/documents/s=965/ddj9601h/9601h.htm* Esistono inoltre 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 s*mart 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: mentre queste note vengono licenziate (estate 2003) è fresco il ricordo del virus BugBear, che presenta svariate caratteristiche utili ad un attacco alla segretezza delle chiavi private.

(20) 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.

(21) 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, Il sigillo informatico*, in *Notariato*, 1997; vedasi anche M. MICCOLI, *Commercio telematico: una nuova realtà nel campo del diritto*, in *Riv. dir. impresa,* 1997.

(22) Sul punto M. ORLANDI, *L'imputazione dei testi informatici*, in *Rivista del Notariato*, 1998, p. 867 ss; R. ZAGAMI, *Firma digitale e sicurezza giuridica*, cit, p. 171 ss; A. GENTILI, *Documento informatico e tutela dell'affidamento*, in *Rivista di Diritto Civile*, 1998, II, p. 173.

(23) E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, cit., p. 1139. Non può totalmente escludersi, come già accennato, la possibilità di pensare ad una sorta di conversione formale della firma digitale invalida in quanto tale, in una firma elettronica leggera.

(24) In altezzosa polemica con R. ZAGAMI, *(La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica"*, in *Diritto dell'informazione e dell'informatica*, 1997, p. 903), S. TONDO (*Formalismo negoziale tra vecchie e nuove tecniche*, in *Rivista del Notariato*, 1999, p. 955), nega che la querela di falso sia ipotizzabile in caso di uso abusivo della vera chiave privata, osservando che in simili casi si è dinanzi ad una firma vera. Col che il TONDO trascura forse il fatto che la querela di falso è per giurisprudenza costante (da ultimo, Cass., sez. II, 12 giugno 2000, n. 7975) il rimedio per il caso di abusivo riempimento del biancosegno, *absque pactis*, fattispecie ove l'autenticità della firma non è in discussione. Nella direzione indicata da R. ZAGAMI si è poi infatti unanimemente orientata la dottrina più autorevole, da C. M. BIANCA (*Documento informatico* in *Commentario al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 670) ad A. M. GAMBINO (voce F*irma Digitale*, in *Enciclopedia Giuridica Treccani,* Roma 1999, p. 9), a V. ROPPO (*Il contratto*, in *Trattato di Diritto Privato Iudica/Zatti*, Giuffrè, Milano 2001, p. 240). Ampiamente sul punto M. ORLANDI, *L'imputazione dei testi informatici*, cit., p. 874. L'uso *tout court* abusivo della chiave viene per lo più distinto dall'uso difforme dalle istruzioni del titolare, in relazione al quale il ricorso alla querela di falso non appare possibile: così V. ROPPO, l*oc. ult. cit.*, e C. M. BIANCA, *La firma elettronica: si apre un nuovo capitolo*, in *Studium Iuris*, 2002, p. 1431.

(25) E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, cit., p. 1140: il risultato che si ottiene è esclusivamente lo spostamento della responsabilità in modo quasi esclusivo a carico del titolare della firma, senza risolvere alcuna delle tematiche evidenziate.

(26) Non a caso il legislatore 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 sino a querela di falso, dettò l'articolo 38 della Legge Notarile, imponendo 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 CNN è immediatamente revocata a cura del Presidente Distrettuale in occasione della cessazione dalle funzioni, qualunque ne sia la causa.

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

(28) Operante nel nostro ordinamento come principio di diritto effettivo, scrive C. M. BIANCA, *Commentario al DPR 513/97*, in *Nuove Leggi Civile Commentate*, maggio/agosto 2000, p. 670; sul punto, vedasi anche A. M. GAMBINO, *L'accordo telematico*, Giuffrè, Milano 1997, pag. 234 sgg.

(29) Potrebbe essere utile, ad esempio, una più puntuale definizione delle responsabilità del titolare della firma per la mancata o negligente custodia della *smart card* e dei meccanismi di abilitazione all'uso, quali il PIN.

(30) 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?).

(31) 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.

(32) 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. Di uno sconfinato, quasi commovente ottimismo, dà prova A. PIZZOFERRATO, *La "nuova" firma digitale nell'esperienza giuridica italiana*, in *Contratto e Impresa / Europa,* 2002/1, p. 83, quando afferma che per effetto dell'obbligo legale in capo ai certificatori di "adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri", il rischio di utilizzo abusivo dello strumento da parte di soggetti estranei dovrebbe pressoché azzerarsi. Col medesimo modulo argomentativo, potrebbe affermarsi che grazie all'articolo 2054cc la circolazione stradale non miete pressoché più vittime in Italia da circa sessant'anni, che grazie alla legge 626 gli incidenti sul lavoro sono pressoché scomparsi, e via dicendo.

(33) Se ne trovano alcune tra le *Registration Authorities* che lavorano per la società Infocamere, ad esempio.

(34) 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. Si è appreso in quell'occasione 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.

(35) Arduo negare che ci si trovi dinanzi ad un'illegittimità per eccesso di delega, atteso che le innovazioni introdotte non erano in alcun modo necessarie per attuare la direttiva, e si spingono sino ad un vero e proprio stravolgimento del sistema civilistico delle prove (si veda sul punto G. BUONUOMO, *Lo schema governativo stravolge il processo civile*, in *Interlex,* 24/01/02, *http://www.interlex.it/docdigit/buonomo8.htm)*. M.

CAMMARATA ed E. MACCARONE, *La firma digitale sicura*, Giuffrè, Milano 2003, p. 93, discorrono di principi inaccettabili e di disastro normativo.

(36) Del medesimo avviso P. RICCIUTO, *La "nuova" efficacia probatoria della firma digitale*, *Interlex* 14/02/02, *http://www.interlex.it/docdigit/ricchiu5.htm.* Nessun problema per la firma digitale del CNN, ove l'identificazione è affidata al Presidente Distrettuale.

(37) G. DALLA RIVA, *I mille problemi della firma digitale (2), Interlex,* 31/1/02, *http://www.interlex.it/docdigit/dallariva2.htm*, benché l'espressione usata dal legislatore del T.U. (articolo 9 del DPR 10/11/1997 N. 513, ora articolo 28 DPR 28/12/2000 n. 445) a proposito dell'identificazione del certificatore, "con certezza", sembri suggerire il dovere di un'indagine assai più rigorosa di quella che si viene profilando sul mercato, per ovvie esigenze di costi. Si noti poi che tale obbligo di identificazione, dopo l'attuazione della Direttiva, continua a sussistere solo per le firme digitali e le altre firme basate su certificato qualificato (articolo 11 comma 3 D.Lgs. 10/2002; allegato II lettera d della Direttiva 93/1999), mentre non è previsto per la firma elettronica semplice.

(38) E' davvero significativo come tale critica sia ben presente anche alla dottrina statunitense: si veda ad esempio B. BIDDLE, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, in *San Diego Law Review* (33) 1143, 1996. Atteso che il *Notary Public* americano (a differenza dei notai di quasi tutti gli altri Paesi del mondo, e degli stessi *Civil Law Notaries* statunitensi) è responsabile solo dell'identificazione del sottoscrivente, è parso logico al legislatore dello Utah equiparare i documenti sottoscritti digitalmente a quelli autenticati dal *Notary Public*. BIDDLE osserva invece che la sottoscrizione dinanzi al *Notary Public* 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 pericolosa l'equiparazione operata dalla legislazione dello Utah.

(39) E' lo scenario noto tra i cultori di Internet Law 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.

(40) Severissimo a tal proposito il giudizio di J.K. WINN, *The Emperor's …*, cit, che per una pluralità di ragioni ritiene tuttora impraticabile il tentativo di collegare un'identità descritta in un certificato di firma digitale con l'intenzione della parte ivi indicata di essere considerata giuridicamente vincolata dai contenuti di un documento elettronico *(tie an identity described in a digital signature certificate with the intention of the identified party to be bound to the contents of an electronic record)*.

(41) 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).

(42) Vedasi ad esempio S. TONDO, *op. cit.*, c. 212, che annuncia senza infingimenti: Non interessa l'aspetto tecnologico, con ciò rinunciando tra l'altro a cogliere la questione più attuale e controversa, da un punto di vista puramente giuridico, e specialmente notarile, della materia da lui trattata (l'autenticazione di scrittura elettronica): quali atti si possano validamente autenticare in forma digitale, quali no e perché. Questione, si ripete, giuridica e non tecnica, atteso che dal punto di vista informatico qualunque *file* (anche una fotografia od uno spezzone video) sono suscettibili di firma senza difficoltà alcuna. Per analoghe ragioni anche altri problemi sfuggono all'analisi dell'Autore: ad esempio, non si apprende che il documento autenticato digitalmente dal notaio ha una durata limitata nel tempo, né come si possa a ciò ovviare. Per tacere poi di altre questioni minori: come si realizzi, per essere giuridicamente valido, il collegamento tra l'autentica ed il testo autenticato;

se sia possibile, ai sensi della legge notarile, allegare ad un documento cartaceo un documento elettronico (una procura, ad esempio) …

(43) Per quanto concerne la funzione notarile, è persino troppo ovvio che gli unici casi ammissibili di sostituzione sono il coadiutorato e la delega di cui alla Legge Notarile.

(44) 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.

(45) Sulle orme di W. FLUME (*Allgemeiner Teil des bürgerlichen Rechts, II, Springer, Berlin et al.* 1979, p. 776), 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.

(46) 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.

(47) 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 … (Gabriello PIAZZA, *Negozio sotto nome altrui*, in *Enciclopedia del Diritto*, XXVIII, Giuffrè, Milano 1978, p. 133).

(48) C.M. BIANCA, *Commentario al DPR 513/97*, in *Nuove Leggi Civile Commentate, maggio/agosto 2000*, p. 670.

(49) Per cui vedasi, con brillanti argomentazioni, M. DOLZANI, *infra,* capitolo 4.

(50) Tra le altre, Cassazione, Sezione V Penale, 5 luglio 1990, in *Foro Italiano*, II, c. 436.

(51) E. SANTANGELO e M. NASTRI, *Firme elettroniche e sigilli informatici*, cit., p. 1140. Nel medesimo senso lo studioso cileno (anch'egli notaro) E.A. GAETE GONZÁLES, *Instrumento público electrónico, Bosch, Barcelona,* 2002 2, p. 135. Problemi inesplorati per il diritto è la definizione di D. MINUSSI, Documento elettronico, firma digitale: crepuscolo o rinascimento del notariato? In *Rivista del Notariato*, 2002, p. 1448. 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. Un accostamento può tentarsi alla pubblicità con mezzi idonei della revoca della procura, articolo 1396 cc, anche se qui il fenomeno incide sull'esistenza stessa del documento, non sulla riferibilità a questo o quel soggetto. Difficile da qualificare pure l'esatta natura dei Manuali Operativi, 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 e quindi, ad esempio, dell'attestazione della qualità di notaio in esercizio intrinseca, a termini del Manuale Operativo, alla certificazione operata dal Consiglio Nazionale del Notariato.

(52) A. DE MARSICO, voce *Falsità in atti, Enciclopedia del Diritto*, XVI, Giuffrè, Milano 1967, p. 572.

(53) I. GIACONA, *Appunti in tema di falso c.d. consentito e in atti invalidi,* in *Foro Italiano*, 1993, II c. 436.

(54) E. GRANDE, voce *Falsità in atti, Digesto Penale*, V, UTET Torino 1991, p. 61

(55) Il Tribunale di Cremona (sentenza 16 giugno 1998, in *Cassazione penale*, 1999, 995, con nota di F. NUZZO) si è trovato a decidere in sede penale sul caso di un titolare di tessera Bancomat che aveva denunziato alcuni prelievi abusivi. Le videoregistrazioni eseguite dalla Banca consentirono di stabilire che il responsabile era il figlio del titolare, il quale aveva evidentemente potuto procurarsi il PIN in ambito familiare. Il padre fece luogo a remissione della querela, senza con ciò impedire il giudizio trattandosi di reato perseguibile d'ufficio. Le peculiarità del caso e le specificità tecniche dell'ambito penalistico hanno ovviamente influito sui giudici cremonesi, ma è cionondimeno interessante che si dia soluzione favorevole all'imputato argomentando dall'esistenza, già al momento dei fatti contestati, di un'autorizzazione - tacita, ma non per questo meno significativa - all'utilizzazione di tale tessera all'interno della famiglia.

(56) Così V. ROPPO, *op. loc cit*.

(57) Evoca uno scenario di tal fatta B. SCHNEIER, *Bad Signs*, in *The Industry Standard*, ottobre 2000.

(58) Anche negli USA la diffusione della firma elettronica è rallentata dalla perdurante incertezza sui possibili orientamenti di una corte americana chiamata a decidere in simili contesti: tale lettura è ormai fatta costantemente propria anche dall'informazione non specialistica, ad esempio E.A. TAUB, *Ease of Paperless E-Mail Sidelines the Forlorn Fax,* in *The New York Times*, 13 marzo 2003, ripreso l'indomani dall'*International Herald Tribun*e con il titolo Ease of e-mail sidelines the fax. Feroce la 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).