FIRMA DIGITALE, DOCUMENTO ELETTRONICO E *LEX ATTESTATIONIS*: UN NUOVO (CIRCOSCRITTO) CASO DI DÉPEÇAGE?

Ugo Bechini - giugno 2011

Questo breve lavoro deve molto alle riflessioni collettivamente svolte negli anni sia nella Commissione Informatica del notariato italiano, sia nel New Technologies Working Group *del notariato europeo; ringrazio in particolare i Colleghi Sabrina Chibbaro e Michele Nastri per l'aiuto ricevuto*.

SOMMARIO

1 DEFINIZIONE DELL'OGGETTO : LA FIRMA DIGITALE
2 UNA BREVE INCURSIONE NELLA TECNOLOGIA
3 ALCUNE CONSEGUENZE GIURIDICHE
4 CONFLITTI DI LEGGI: UN TENTATIVO DI RICOSTRUZIONE
- 4.1 Scadenza, sospensione e revoca
- 4.2 I limiti di impiego del certificato
- 4.3 Poteri rappresentativi incorporati nei certificati
- 4.4 La firma/funzione
- 4.5 L'impiego della chiave privata da parte di soggetto diverso dal titolare
  - 4.5.1 L'affidamento volontario
  - 4.5.2 La firma apocrifa
  - 4.5.3 Una considerazione sistemica
- 4.6 La forma
- 4.7 Manipolazioni del documento

5 ASSENZA DI ANALOGIE TRA CERTIFICAZIONE E RUOLO DEL NOTAIO
6 TIMESTAMPING
7 ESTENSIBILITA' DELLE CONCLUSIONI AD ALTRE FIGURE DI FIRMA ELETTRONICA

Se gli scambi internazionali di comunicazioni elettroniche, anche a contenuto giuridicamente rilevante, sono da tempo una realtà, ancora poco significativa è la circolazione internazionale di documenti elettronici provvisti di firma digitale. Concorrono in tal senso almeno due fattori. Da un lato, le applicazioni più importanti della firma digitale non sono in ambito business, ma nei rapporti di cittadini, professionisti ed imprese con le Pubbliche Amministrazioni, e si risolvono per lo più in circuiti chiusi nazionali. D'altro lato, per strano che possa sembrare, solo di rado i softwares di uso comune in un Paese sono in grado di leggere correttamente documenti cui sia stato apposta la firma digitale in un altro Paese.

Non si affronteranno però in questa sede tali problematiche, che sono state peraltro toccate in un precedente lavoro [1], né i problemi connessi alla circolazione degli atti pubblici in forma digitale [2]. Obiettivo di queste righe è invece affrontare il regime internazionalprivatistico in senso stretto dei documenti firmati digitalmente. Si tenterà di dimostrare che la firma digitale conserva un rapporto con l'ordinamento nel cui ambito la firma stessa è stata creata, e che alle norme di tale ordinamento deve essere probabilmente riservato uno spazio nella ricostruzione internazionalprivatistica della fattispecie.

1. DEFINIZIONE DELL'OGGETTO: LA FIRMA DIGITALE

Oggetto d'esame sarà la firma digitale in senso stretto. E' forse opportuna una precisazione terminologica. La nozione generica da cui conviene prendere le mosse è quella di *firma elettronica*: *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*. La definizione è quella dettata dalla legislazione italiana [3], che deriva a sua volta da quella contenuta nella Direttiva Europea 93/1999 [4], e non presenta differenze di rilievo rispetto alle nozioni rinvenibili (ad esempio) nella legislazione federale statunitense [5], nel modello di

---

1 *A New approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions,* con D. GASSEN, in *Michigan State Journal of International Law*, volume 17 (2008/2009) Issue 3. L'articolo è stato pure pubblicato in traduzione italiana (*Firme elettroniche a valore legale internazionale: un nuovo approccio per migliorare l'interoperabilità*) ne *Il diritto dell'informazione e dell'informatica*, n. 2/2009, p. 349. Una sintesi in lingua tedesca (*Verifikationsplattform für elektronische Signaturen*) è apparsa in *Datenschutz und Datensichereit*, 2008, p. 673

2 Su cui un accenno infra, § 4.4.

3 DLgs 7/3/05 n. 82, articolo 1 comma 1.

4 Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (GUCE L 13 19/1/2000).

5 Public Law 106 - 229 - Electronic Signatures in Global and National Commerce Act, 30 giugno 2000.

legge uniforme per gli stati USA, detta UETA [6], in quella cinese [7] e nella Model Law dell'UNCITRAL [8]. Si tratta di una nozione assai ampia, cui sono riconducibili figure assai disparate. Persino un SMS, secondo un'opinione [9] che pare a chi scrive convincente, può considerarsi un documento firmato elettronicamente: si tratta pur sempre di un dato elettronico (il testo) associato ad altro dato elettronico (il numero mittente), che serve ad identificare la provenienza del messaggio.

All'interno del genus "firma elettronica" possono riconoscersi diverse species. La prima tipologia nota, ma tuttora la più completa ed affidabile, è la *firma digitale*. Non in tutti gli ordinamenti è dato rinvenirne una definizione diretta. In una prima fase i legislatori hanno in effetti disciplinato la sola firma digitale: fu ad esempio il caso del primo testo in materia al mondo, quello dello Utah, del 1995 [10], e del primo europeo, la legge italiana del 1997 [11]. Nel prosieguo ha frequentemente prevalso il punto di vista secondo cui la firma digitale è solo una tecnologia come un'altra, destinata magari ad essere rapidamente ed imprevedibilmente soppiantata: di qui l'inopportunità di una sua esclusiva consacrazione legislativa. In alcuni casi [12] si si è deciso quindi di dettare la sola definizione di firma elettronica. La direttiva europea ha optato per una soluzione più complessa, disegnando a tavolino altre due nozioni (firma elettronica avanzata e firma elettronica qualificata) che corrispondono a crescenti livelli di affidabilità: lo ha fatto, però, in una chiave *technology neutral*, senza indicare cioè tecnologie determinate, ma dettando i requisiti astratti cui una tecnologia deve rispondere per poter essere classificata in una delle indicate categorie. Anche dopo l'attuazione della direttiva il legislatore italiano, pur avendo adottato (come è ovvio) le tre nozioni "europee" di firma elettronica semplice, avanzata e qualificata, ha deciso di conservare, armonizzandola nel contesto, una definizione di firma digitale, quale sottotipo della firma avanzata.

La nozione di firma digitale dettata dal legislatore italiano è però molto complessa [13], ed una sua esposizione andrebbe al di là delle presenti esigenze.

---

6 Uniform Electronic Transactions Act (1999), National Conference of Commissioners on Uniform State Laws.

7 Legge della Repubblica Popolare Cinese sulle firme elettroniche, promulgata il 28 agosto 2004.

8 Model Law on Electronic Signatures (MLES) dell'United Nations Commission on International Trade Law, 2001. http://www.uncitral.org; se ne trova un commento in F. J. GARCIA MÁS, *Comercio y firma electrónicos*, Lex Nova, Valladolid 2004, p. 315.

9 S. MASON, *Electronic Signatures*, LexisNexis, London 2003, p. 101.

10 Il Digital Signature Act (Utah Code, Title 46, Chapter 3).

11 DPR 10/11/1997 n. 513 (GU 13/03/1998 n.60).

12 E' il caso dei testi normativi citati alle note da 5 ad 8.

13 L'attuale definizione (DLgs 30/12/10 n. 235, articolo 1) è: *un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite*

Indipendentemente dall'esistenza di una nozione legislativa in questo o quel Paese, la firma digitale è però figura ovunque nota in termini ampiamente sovrapponibili. La si può sinteticamente definire come un sistema basato sulla crittografia asimmetrica e sull'intervento di un terzo certificatore, che consente di attribuire un documento ad un soggetto determinato e di accertare che il messaggio non è stato oggetto di manipolazioni.

Ciò non toglie che alcune considerazioni possano trovare applicazione ad altre tipologie di firma elettronica, ma su questo si ritornerà al termine di queste brevi note. Dedichiamo ora pochissime righe alla tecnologia della firma digitale [14].

---

la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Al sistema di chiavi si accennerà al §2, occorre invece richiamare la nozione di certificato qualificato: *certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva*. I due allegati citati sono i seguenti:

ALLEGATO I - Requisiti relativi ai certificati qualificati

I certificati qualificati devono includere:

a. l'indicazione che il certificato rilasciato è un certificato qualificato;
b. l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;
c. il nome del firmatario del certificato o uno pseudonimo identificato come tale;
d. l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;
e. i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;
f. un'indicazione dell'inizio e del termine del periodo di validità del certificato;
g. il codice d'identificazione del certificato;
h. la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;
i. i limiti d'uso del certificato, ove applicabili; e
j. i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

ALLEGATO II - Requisiti relativi ai prestatori di servizi di certificazione che rilasciano certificati qualificati

I prestatori di servizi di certificazione devono:

a. dimostrare l'affidabilità necessaria per fornire servizi di certificazione;
b. assicurare il funzionamento di un servizio di repertorizzazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;
c. assicurare che la data e l'ora di rilascio o i revoca di un certificato possano essere determinate con precisione;
d. verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato;
e. impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e i gestione adeguati e corrispondenti a norme riconosciute;
f. utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;
g. adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza nel corso della generazione di tali dati;
h. disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione;

2. *UNA BREVE INCURSIONE NELLA TECNOLOGIA*

La firma digitale deriva, alquanto curiosamente, da una tecnica di criptazione. La comprensione di alcuni tratti salienti di questa tecnologia, ad avviso di chi scrive, è indispensabile ai fini di un corretto inquadramento giuridico della fattispecie.

Particolari tecniche matematiche, basate principalmente sulle proprietà dei numeri primi, consentono di creare sistemi di criptazione asimmetrica. In altri termini: la chiave che permette di criptare un messaggio e la relativa chiave di decriptazione sono distinte e non è possibile risalire da una all'altra [15]. L'applicazione di tipo propriamente crittografico è concettualmente interessante. Una stazione militare che debba ricevere messaggi criptati dalle proprie unità potrà ad esempio diffondere pubblicamente la chiave di criptazione, e poco importa che anche il nemico se ne impadronisca: i messaggi potranno infatti essere letti solo da chi possiede la corrispondente chiave di decriptazione, che come detto non può essere

---

i. tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;
j. non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave;
k. prima di avviare una relazione contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e i risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
l. utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:
   - soltanto le persone autorizzate possano effettuare inserimenti e modifiche;
   - l'autenticità delle informazioni sia verificabile,
   - i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato,
   - l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

14 Se ne trovano esposizioni dettagliate ma ben accessibile ai giuristi, cui sono destinate, nel fondamentale lavoro di R. ZAGAMI, *Firma digitale e sicurezza giuridica*, CEDAM, Padova 2000, ed in M. CAMMARATA ed E. MACCARONE, *La firma digitale sicura*, Giuffré, Milano 2003; entrambi I testi rappresentano però soprattutto un sicuro punto di riferimento per chi voglia accostarsi allo studio di questa figura dal punto dei vista giuridico. Una tuttora validissima trattazione di taglio soprattutto tecnico è invece quella di W. FORD e M. S. BAUM, *Secure Electronic Commerce*, Prentice Hall, Upper Saddle River (New Jersey, USA) 2001.

15 Nei sistemi a chiave simmetrica le operazioni di criptazione e decriptazione sono invece affidate a chiavi ricavabili l'una dall'altra. Si pensi al più semplice dei codici, quello che consiste nel sostituire ogni lettera con quella che la precede nell'ordine alfabetico. IBM, ad esempio, diverrà HAL (così si chiamava, non a caso, il supercomputer ribelle di *2001 Odissea nello Spazio*). Criptazione e decriptazione sono processi simmetrici, e chi ha accesso ad uno ha necessariamente accesso all'altro. Esistono codici a chiave simmetrica immensamente più complicati, come il celeberrimo Enigma, utilizzato dalle forze armate tedesche durante la Seconda Guerra Mondiale, ma il principio di fondo resta sostanzialmente il medesimo.

ricavata dalla prima [16].

Per sfruttare questa tecnica al fine dell'apposizione di una firma è sufficiente un semplice accorgimento: invertire l'uso delle chiavi. La chiave di criptazione verrà dunque conservata riservatamente dal mittente (la chiameremo quindi chiave segreta, o privata) mentre la chiave di decriptazione sarà posta a disposizione di chiunque, tipicamente su Internet: la chiameremo quindi chiave pubblica. Il mittente cripterà il messaggio con la sua chiave segreta ed invierà al destinatario sia il messaggio in chiaro che il messaggio criptato, che ai presenti fini possiamo per semplicità chiamare firma [17]. Il destinatario si procurerà la chiave pubblica del mittente e decripterà il messaggio. Se il testo [18] così ricavato corrisponde a quello trasmesso in chiaro, due cose sono accertate:

- il testo proviene dal detentore della chiave segreta, l'unica in grado di produrre firme decriptabili con la corrispondente chiave pubblica;
- il testo non è stato alterato: un eventuale impostore potrebbe falsificare a suo piacimento il messaggio in chiaro ma, non possedendo la chiave segreta, non sarebbe in grado di produrre la firma corrispondente. In tal caso, come suol dirsi, fallirebbe la verifica della firma.

3. ALCUNE CONSEGUENZE GIURIDICHE

Da questa succintissima illustrazione si possono trarre due gruppi di osservazioni.

In primo luogo: la firma digitale, di per sé non costituisce (come la tradizionale firma autografa) la traccia storica del contatto tra un soggetto ed un documento. Si tratta invece della componente di una fattispecie che si articola, tipicamente, su quattro passaggi logici [19]:

1. la tecnologia consente di dimostrare che un certo testo, in quanto decrittabile con una determinata chiave pubblica, è stato creato con la corrispondente chiave segreta. Le possibilità di violare le fondamenta matematiche di tale sistema appaiono estremamente ridotte [20];

---

16 Questa caratteristica dei sistemi a chiave asimmetrica, del tutto controintuitiva, indusse i responsabili dei servizi segreti britannici, nei cui laboratori era stata fatta la scoperta, ad accantonarli: si temeva contenessero una falla sfuggita agli analisti. La storia è narrata da S. LEVY in *Crypto: how the code rebels beat the government, saving privacy in the digital age*, Viking, New York 2001, p. 313.

17 Nella pratica in verità si introduce a questo punto un ulteriore passaggio tecnico, il cosiddetto *hashing*, ininfluente però ai nostri circoscritti fini.

18 Si parla per semplicità di *testo*, ma in realtà può trattarsi di qualunque file.

19 SI veda sul punto M. ORLANDI, *Il falso digitale*, Giuffrè, Milano 2003, soprattutto a p. 61.

20 Le congetture intorno alla potenza di calcolo necessaria per violare i sistemi di crittografia asimmetrica sono peraltro alquanto inaffidabili: nel 1977 si ipotizzava che la chiave RSA129 avrebbe resistito per

2. un soggetto detto certificatore (o Certification Authority) [21], dichiara che la corrispondente chiave segreta si trova in un determinato dispositivo di firma, detto *token*: normalmente si tratta di una *smart card* [22];
3. un soggetto detto Registration Authority [23], dichiara di aver consegnato quel *token* ad una determinata persona, che sarà identificata in un documento pubblicato on line dalla Certification Authority, detto *certificato* [24];
4. è nella responsabilità del titolare impedire che la chiave segreta di firma cada in mani altrui.

In alcuni sistemi giuridici [25] si rivengono norme ad hoc che imputano i documenti firmati digitalmente alla persona indicata dal certificato: con ciò si pone in essere una tecnica virtuale di produzione di effetti giuridici, una *fictio* [26] che scavalca con un'unica arcata i quattro passaggi logici sopra indicati. In tal caso, la firma digitale (pur continuando a non offrire alcuna prova dell'azione di un soggetto determinato)

---

alcuni miliardi di anni, mentre nel 1992 si rivelarono sufficienti otto mesi di lavoro: S. LEVY, *op. cit.*, p. 273. Le chiavi attuali sono enormemente più sicure, ed il progressivo aggiornamento dei softwares sembra mantenere costante una sana distanza di sicurezza tra le soluzioni crittografiche in uso e gli aspiranti pirati. Chi fosse interessato a violare una chiave di firma, troverà in genere assai più semplice ed economico corrompere un collaboratore, od intercettare da un ambiente vicino gli impulsi elettromagnetici emessi dalla tastiera, onde scoprire il PIN della smart card prima di procedere alla sua sottrazione: avvalersi, insomma, delle "normali" tecniche di spionaggio industriale. Da tempo si ipotizza però che dispositivi di *quantum computing* possano consentire attacchi alle fondamenta matematiche del sistema. L'eventualità, sinora presentata in chiave teorica, appare oggi più concreta con la consegna alla Lockheed del primo computer che impiega tale tecnologia, nella primavera 2011: T. SIMONITE, *Tapping Quantum Effects for Software that Learns*, 1 giugno 2011, MIT Technology Review (www.technologyreview.com).

21 Che può essere un operatore commerciale come pure un soggetto pubblico.

22 Un oggetto dall'aspetto di una carta di credito.

23 Che può anche coincidere con la Certification Authority.

24 Si deve appena osservare che oggetto del certificato è la chiave pubblica, non il singolo documento firmato: il certificato può essere quindi utilizzato per una serie indefinita di documenti, senza che il certificatore debba o possa esserne a conoscenza.

25 Quello italiano, ad esempio: si veda a nota 59. La dottrina anglosassone pare indirizzata in tutt'altra direzione. L'americana 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), ritiene 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*). Nello stesso senso l'inglese S. MASON, *op. cit.*, p. 486 e soprattutto p. 348: *No form of electronic signature is capable of linking the use of a signature to a particular person. Unless the sending party confirms they sent the message or document with the signature attached, the recipient cannot determine whether the sending party authorized the use of the signature* (nessuna firma elettronica può collegare l'uso della firma ad una determinata persona. A meno che il mittente non confermi d'aver inviato il messaggio firmato, il destinatario non può stabilire se il mittente ha autorizzato l'uso della firma).

26 Sull'impiego della fictio nel trattamento legislativo delle nuove tecnologie si veda V. GAUTRAIS, *Fictions et présomptions: outils juridiques d'intégration des technologies*, conferenza tenuta il 30 settembre del 2002 alla Faculté de droit dell'Università di Montréal, la cui trascrizione è disponibile presso www.lex-electronica.org.

permette un'imputazione nominale che discende dall'operatività della catena basata sui quattro anelli cui si è fatto cenno. Come ogni catena, anche questa (si tende troppo spesso a dimenticarlo) non potrà essere più solida del più debole dei suoi anelli, che sono di varia natura: tecnologico il primo, industrial/organizzativo il secondo, affidati alla comune umana diligenza i restanti due.

In secondo luogo la firma digitale non si sostanzia in un segno comunque riferibile ad una persona: si tratta di un documento in forma criptata [27]. Da un lato, quindi, la firma varia al variare del testo firmato. D'altro lato la firma, di per sé, è una sequenza di caratteri che non contiene alcuna informazione od indizio intorno al suo autore [28]. Solo decriptando la firma con la corretta chiave pubblica, fornita dal certificatore, si potrà attribuire (nel peculiare senso appena specificato) il documento al titolare del certificato.

Di qui una prima fondamentale conclusione. La firma digitale non è, a differenza di quella autografa, il prodotto diretto di un comportamento umano che la legge (*una* legge, in prospettiva internazionalprivatistica) possa apprezzare, qualificare e disciplinare di per sé. Si tratta invece di una fattispecie giuridica complessa che deriva tipicamente dall'azione combinata e regolamentata di diversi soggetti, tra cui titolare del certificato e certificatore [29]. **La firma digitale è insomma un prodotto del diritto, non (solo) un oggetto del diritto medesimo**. In sé, come si è osservato, non è altro che una sequenza di caratteri priva di senso alcuno; acquista un significato solo nell'ambito di un'appropriata interazione tra più soggetti. Ciò che rende in ultima analisi peculiare, sotto il profilo internazionalprivatistico, la firma

---

27 Assomiglierà a qualcosa del tipo *CB0B088DAACDC404542063JD3M337EC940610A63DB9B4DJ213BI492362E19953C2FC7902089D936E850C195BF9I0DBBF09FD0930EA535A4BF863MF0K8I.* Come si vede, nulla che abbia significato per un essere umano (e, se è per questo, neppure per una macchina), senza l'intervento di un certificatore.

28 Qui si parla della firma in senso stretto. Abitualmente, le firme digitali sono collocate in plichi informatici che contengono anche il certificato, a sua volta firmato digitalmente dal certificatore. Qualora si conosca già la chiave pubblica del certificatore, non vi sarà dunque bisogno di collegarsi online col certificatore, se non per verificare se il certificato non sia stato nel frattempo revocato. Ciò non sposta però minimamente i termini della questione, giacché la firma sarà comunque interpretata alla luce delle informazioni fornite dal certificatore; è irrilevante che queste siano rese disponibili all'utente finale insieme alla firma o debbano essere acquisite separatamente. Neppure importa, d'altra parte, che la decisione di prestar fede ad un determinato certificatore sia stata preventivamente assunta dall'utente finale in via generale, o volta per volta. Se vi è un profilo di criticità, risiede piuttosto nel fatto che in alcuni softwares sono preinstallate all'origine le chiavi pubbliche di determinati certificatori, scelti dal produttore del software per ragioni perlopiù commerciali. Un utente non particolarmente accorto potrebbe erroneamente immaginare che le verifiche eseguite su tali basi siano il frutto di indiscutibili verità scientifico/informatiche, anziché discendere dalla vulnerabile catena logica descritta nel testo.

29 La tecnologia della firma digitale a chiavi asimmetriche può essere impiegata anche senza l'intervento di un terzo certificatore: è il caso dei certificati *self-signed,* o di quelli basati sulla cosiddetta *chain of trust*, come PGP, su cui si veda FORD E BAUM, *op. cit.*, p. 275. Tale ipotesi è però al di fuori dell'ambito del presente lavoro, come definito al § 1.

digitale, è che questa non si basa su un rapporto diretto tra autore del documento ed il suo fruitore, ma attribuisce un fondamentale ruolo ad un terzo: il certificatore.

L'attività del certificatore, da parte sua, non si svolge in uno spazio vuoto di diritto. Al contrario, è inquadrata in un'elaborata cornice giuridica:

- rileva innanzitutto la legge cui il certificatore è sottoposto, e che non di rado fissa regole che disciplinano la sua azione [30];
- vi è poi il contratto tra il certificatore ed il cliente, che tipicamente sarà sottoposto alla legge di cui al punto precedente, e sarà a sua volta fonte di reciproche obbligazioni;
- *last but not least*, il cosiddetto *Certification Practice Statement* (CPS) [31] tradotto per lo più in italiano come *Manuale Operativo*. La dizione italiana esprime in maniera decisamente insufficiente la natura e la funzione di tale testo. Si tratta di un documento, tipicamente pubblicato sul sito web del certificatore, con il quale quest'ultimo enuncia le procedure seguite nell'attività di certificazione. Da un lato, i terzi possono fare affidamento sul CPS per conoscere il livello di attendibilità del certificato e, di conseguenza, delle firme emesse in base ad esso; d'altro lato, delimita la responsabilità del certificatore stesso.

Un esempio potrà forse aiutare ad immaginare quali problematiche siano insite in questa architettura. Il Finanzgericht di Münster si è trovato nel 2006 a decidere [32] su un ricorso firmato digitalmente sulla base di un certificato che prevedeva un limite massimo di utilizzo pari a cento euro: atteso che la controversia era di importo superiore, il ricorso venne considerato irricevibile. Il Bundesfinanzhof [33] ribaltò alcuni anni più tardi la decisione di primo grado, statuendo che il limite di cento euro doveva intendersi applicabile solo a transazioni a carattere finanziario, e non a vicende come quella oggetto della decisione.

Nell'esperienza internazionale i limiti monetari di impiego del certificato sono perlopiù collegati alle modalità dell'identificazione del titolare: a modalità meno affidabili (pensiamo a rilasci interamente *online*) corrispondono limiti d'uso inferiori, da cui discende una più ridotta responsabilità del certificatore. Alcuni certificatori

---

30 Si vedano ad esempio, per l'Italia, gli articoli 26 ss. del DLgs 7/3/05 n. 82.

31 Si vedano a tal proposito le regole contenute nel documento noto come RFC3647, http://tools.ietf.org/html/rfc3647 e l'amplissima trattazione di FORD e BAUM, *op. cit.*, p. 385ss.

32 FG Münster, 13.10.2006 - 11 K 3833/05 AO (EFG, 2007, 55).

33 Urteil vom 19.2.2009 - IV R 97/06.

emettono anzi certificati di classi diverse [34], cui corrispondono modalità di identificazione di crescente rigore e limiti d'uso progressivamente più elevati.

E' difficile immaginare che dalla disciplina dei limiti d'utilizzo si possa prescindere anche laddove il certificato venga utilizzato per un contratto sottoposto ad una legge diversa dalla legge nel cui ambito è stata rilasciata la certificazione, e che propongo di chiamare *lex attestationis* [35]. Se le modalità di rilascio di una firma digitale sono infatti reputate, nel sistema di provenienza, idonee ad impieghi sino ad un determinato valore, disconoscere tali limiti quando al negozio sottoscritto sia applicabile un'altra legislazione significherebbe introdurre in alcuni casi discrasie inaccettabili. Il problema non è però (banalmente) il rischio di dare accesso a documenti inaffidabili: in una prospettiva internazionalprivatistica, ben può reputarsi fisiologico che un ordinamento reputi idonea una tipologia documentale rifiutata da un altro. La questione è più specificamente legata alla natura giuridica della firma digitale, ed in particolare alla concatenazione di fenomeni giuridici su cui riposa. Si finirebbe, in particolare, col considerare un terzo tenuto a fare affidamento sulla bontà di una firma, senza che egli possa contare sulla responsabilità del certificatore qualora il certificato risultasse inattendibile, facendo luogo ad una rottura della sequenza (logica, giuridica ed economica) su cui si fonda il valore legale della firma digitale. Uno squilibrio che ben si potrebbe definire sistemico, e di cui va verificata con attenzione la tollerabilità.

4. *CONFLITTI DI LEGGI: UN TENTATIVO DI RICOSTRUZIONE*

Vi sono insomma elementi che spingono ad indagare se nella ricostruzione a fini internazionalprivatistici delle fattispecie documentali provviste di firma digitale vi sia spazio per l'applicazione della *lex attestationis*. Si tratta di una questione che non trova equivalente nel trattamento della firma autografa che, come tutte le *solennités écrites*, è considerata *question de forme par excellence* [36] e dunque senz'altro sottoposta alla legge che regola la forma dell'atto. L'indagine, si anticipa subito,

---

34 Dal sito (consultato nel maggio 2011) del celeberrimo certificatore californiano VeriSign, leader del settore: *To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit VeriSign's and the applicable Affiliates' liability outside the context of the NetSure Protection Plan. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting VeriSign's and the Affiliate's damages concerning a specific Certificate: Class 1, One Hundred U.S. Dollars ($ 100.00 US); Class 2, Five Thousand U.S. Dollars ($ 5,000.00 US); Class 3, One Hundred Thousand U.S. Dollars ($ 100,000.00 US).* Degno di nota il tetto massimo di 100.000 dollari, inferiore (nel giugno 2011) ai 75.000 euro.

35 Ringrazio per l'aiuto ricevuto sul punto il Professor Ferruccio Bertini, Ordinario di Letteratura Latina presso l'Università di Genova.

36 La formula è di H. BATTIFOL e P. LAGARDE, *Droit International Privé*, Librairie générale de droit et de jurisprudence, Paris 1983, p. 325.

riserverà alla *lex attestationis* un ruolo assai modesto. Occorre comunque distinguere diversi profili del fenomeno.

4.1 - *Scadenza, sospensione e revoca*

La vigenza del certificato dovrà essere valutata secondo la *lex attestationis*, nel cui contesto andranno in particolare apprezzate in particolare scadenza, sospensione e revoca [37]. Non pare possibile infatti dare il corretto rilievo a tali vicende se non nel quadro giuridico in cui maturano i relativi vincoli giuridici e contrattuali, che determinano i limiti cronologici entro i quali il certificato resta attendibile, e definiscono (talora in dettaglio!) compiti e responsabilità del certificatore e del titolare. Non sembrano invece sussistere ragioni sufficienti per sottrarre all'ambito operativo della legge che governa la forma del documento, la disciplina degli effetti che discendono da tale mancata vigenza.

La distinzione può avere ad esempio notevole importanza in relazione ad un tema dibattuto: gli effetti della scadenza del certificato. In alcune culture giuridiche, come quella italiana, prevale l'idea secondo cui tale evento travolge la validità delle firme già apposte, a meno che non si possa provare [38] l'anteriorità della firma rispetto alla scadenza stessa [39]. In altri Paesi, come ad esempio la Germania [40], si ritiene perlopiù che a partire dal momento di scadenza del certificato le firme subiscano una sorta di lenta erosione del loro status giuridico, restando però in linea di principio valide. Si può quindi immaginare che una firma digitale di cui non sia possibile dimostrare l'anteriorità rispetto alla scadenza del certificato, sia da considerarsi in linea di principio valida se apposta ad esempio ad un contratto governato, per quanto riguarda la forma, dalla legge tedesca, ed invalida se la legge che regola la forma è quella italiana. Fermo restando che potremo invece apprezzare se il certificato abbia perduto o meno la sua validità (e quando) solo nel quadro della *lex attestationis.*

4.2 - *I limiti di impiego del certificato*

Analogo approccio ritengo debba proporsi per i limiti di impiego del certificato, siano essi qualitativi (limitino cioè l'uso della firma a determinate tipologie di documenti) o quantitativi (laddove cioè il limite sia per importo dell'operazione cui la

---

37 Si vedano in argomento ZAGAMI, *op. cit.*, p. 109 ss. e FORD e BAUM, *op. cit.*, 216 ss.

38 Ricorrendo al timestamping (su cui al § 6) od altre idonee soluzioni, come la documentabile immissione in un'infrastruttura di conservazione controllata.

39 Qualora nuove scoperte matematiche o vistosi incrementi della potenza dei computer (si veda a nota 20) rendessero in futuro possibile falsificare le firme digitali, anche le firme già apposte diverrebbero inaffidabili. Per questo la dottrina italiana prevalente (si veda soprattutto ZAGAMI, *op. cit.*, p. 214) ritiene che la scadenza del certificato sia evento parificabile alla distruzione del documento cartaceo.

40 A. ROSSNAGEL ed altri, *Erneuerung elektronischer Signaturen—Grundfragen der Archivierung elektronischer Dokumente*, 15 *Computer und Recht*, 301–06 (2003); U. PORDESCH e C. FRYE, *Sicherheitseignung von Algorithmen qualifizierter Signaturen*, 27(2) *Datenschutz und Datensicherheit* 73 (2003).

sottoscrizione si riferisce). Se la limitazione pare dover essere regolata dalla *lex attestationis*, gli effetti della violazione del limite restano verosimilmente disciplinati dalla legge che regola la forma del documento. Laddove infatti in base a quest'ultima legge si debba ritenere idonea anche una firma emessa in violazione del limite [41] (e quindi non assistita, od assistita solo in parte, dalla responsabilità del certificatore) non v'è apparente ragione per cui tale giudizio di valore, che è evidentemente raccordato alla funzione che il documento svolge nell'ordinamento in cui è destinato ad operare, debba cedere il passo a quello proprio dell'ordinamento di provenienza della firma stessa. Occorrerà però, come già si osservava al § 3, considerare attentamente se l'ordinamento che regola la sostanza dell'atto possa tollerare l'operatività di firme non assistite dalla responsabilità del certificatore, e che rischiano quindi di lasciare sforniti di tutela i terzi.

4.3 - *Poteri rappresentativi incorporati nei certificati*

La *lex attestationis* disciplinerà altresì le vicende connesse ai poteri rappresentativi incorporati nei certificati. Occorre qui introdurre una distinzione. Ben può darsi che un rappresentante (organico, legale o volontario, poco importa) operi in ambito elettronico una tradizionale *contemplatio domini*. Potrà in altri termini avvalersi di un certificato a lui personalmente rilasciato per sottoscrivere un documento nel cui corpo sia individuato il soggetto rappresentato. Può accadere invece che al rappresentante sia rilasciato un apposito certificato [42] che reca menzione del potere rappresentativo, e la firma digitale sia apposta ad un documento direttamente riferibile al rappresentato [43]. L'ipotesi, come si vede, contiene elementi di notevole criticità. Su quali basi il certificatore, rilasciando il certificato, dichiara sussistere il potere rappresentativo? Sulla base di una semplice dichiarazione del rappresentante o sulla scorta di una verifica obiettiva ed indipendente? Ed ancora ci si può chiedere quali meccanismi siano adottati onde assicurare che, in caso di cessazione dei poteri di rappresentanza, il certificato venga tempestivamente revocato. Le risposte variano a seconda delle circostanze e degli ordinamenti di

---

41 Come ha fatto la giurisprudenza tributaria tedesca nel caso citato alla nota 33.

42 In alternativa, le informazioni relative al rapporto rappresentativo possono essere contenute (come altre) in un certificato distinto, detto Certificato di Attributo, collegato al certificato principale. Mentre quest'ultimo identifica la persona, il primo certifica le sue prerogative: il rapporto tra certificato principale e quello d'attributo è stato paragonato al rapporto tra passaporto e visto. Diviene così possibile gestire indipendentemente identità e prerogative: la cessazione da una carica, ad esempio, comporterà la revoca del certificato di attributo da non di quello principale. Il rilascio di un certificato di attributo è poi operazione assai più semplice del rilascio di un certificato di firma. Si tratterebbe di una notevole semplificazione laddove l'impiego della firma digitale fosse generalizzato, ed un numero considerevole di persone si trovasse ad usarla in relazione a più funzioni (ad esempio: avvocato, presidente di un Rotary Club e procuratore dei propri genitori). Atteso che l'uso della firma digitale è invece ad oggi molto circoscritto e specializzato (e tale pare destinato a rimanere), i certificati d'attributo non hanno al momento un impiego significativo.

43 Caso diverso da quello di cui al § 4.5.1, in cui il rappresentante impiega direttamente il certificato del rappresentato col consenso di quest'ultimo.

riferimento. Appare quindi preferibile ritenere che in simili ipotesi la sussistenza del potere rappresentativo venga apprezzata in base alle norme della *lex attestationis*, e dunque in un modo coerente con il livello di accuratezza che tale ordinamento esige per l'inserimento in certificato di siffatte informazioni.

4.4 - *La firma/funzione*

Figura analoga è la firma/funzione [44]: specifici certificati rilasciati a soggetti che ricoprono pubbliche funzioni, e di regola utilizzabili solo in tale ambito. E' il caso, ad esempio, della firma dei notai italiani, primo esempio in Europa del suo genere: il Consiglio Nazionale del Notariato rilascia certificati solo a notai in esercizio [45], e li revoca immediatamente in caso di cessazione dalle funzioni, ed anche in caso di semplice cambio di distretto notarile [46]. Si parla in ipotesi come questa di Autorità di Certificazione piatta, nel senso che tutti i certificati rilasciati da quell'Autorità hanno identico valore: attestano ad un tempo l'identità del titolare ed il possesso da parte sua delle funzioni notarili. Pare evidente che tale peculiare proprietà giuridica di siffatti certificati possa e debba essere apprezzata solo nel quadro della *lex attestationis*.

Si muovono in tale ottica, peraltro, le principali iniziative internazionali dirette ad assicurare la circolazione internazionale dei documenti pubblici, ed in particolare notarili. Il progetto più importante in questo settore è quello della e-Apostille [47], modello infrastrutturale teso a replicare in ambito elettronico la tradizionale Apostille su carta [48]: la natura pubblica del documento è unilateralmente attestata dall'Autorità designata del Paese di provenienza, che applica ovviamente la propria legge (non senza qualche conseguenza paradossale [49]). E così la piattaforma

---

44 M. NASTRI, *Firme elettroniche ed enunciazione di funzioni, qualifiche, poteri. La firma funzione del notaio*, in *Firme elettroniche. Questioni ed esperienze di diritto privato*, Studi del Consiglio Nazionale del Notariato, Giuffrè, Milano 2003, p. 41.

45 Punto 3.3. del Manuale Operativo del Consiglio Nazionale del Notariato (CNN), disponibile all'indirizzo http://ca.notariato.it. Recentemente l'articolo 23bis della legge 16 febbraio 1913, n. 89 (introdotto dall'articolo 1 del DLgs 2 luglio 2010, n.110) ha stabilito che il notaio deve obbligatoriamente ricorrere al sistema di firma del CNN; nella pratica ciò accadeva da svariati anni.

46 Articolo 23ter della legge 16 febbraio 1913, n. 89 (inserito dall'articolo 1 del DLgs 2 luglio 2010, n.110).

47 Si veda il sito http://www.e-app.info.

48 Sulla base della Convenzione dell'Aja del 5 ottobre 1961: si veda all'uopo l'Apostille Section del sito della Conferenza Permanente dell'Aja, http://www.hcch.net.

49 Il 7 ottobre 2010, il Presidente statunitense Barack Obama annunciò il proprio veto all'H.R. 3808, The Interstate Recognition of Notarizations Act of 2010 (disponibile presso la Biblioteca del Congresso, http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.3808:). Tale testo, già approvato da Camera e Senato, prevedeva l'obbligo da parte di tutti gli Stati dell'Unione di riconoscere il valore giuridico degli atti (cartacei od elettronici) autenticati da notaio di altro Stato. La vicenda (su cui si veda il sito della Casa Bianca, http://www.whitehouse.gov/blog/2010/10/07/why-president-obama-not-signing-hr-3808) destò una certa sorpresa fuori dagli USA, ove pochi sospettavano la situazione, soprattutto considerando che, paradossalmente, i Paesi membri della Convenzione dell'Aja sull'Apostille si considerano sostanzialmente vincolati a riconoscere, bon gré mal gré, il valore giuridico degli atti notarili

Bartolus [50], voluta dal notariato europeo, che consente di stabilire in tempo reale se un determinato documento elettronico provenga o meno da un notaio europeo in esercizio. Anche qui, la certificazione della qualità notarile dell'autore del documento è rimessa interamente all'ordinamento in cui il notaio opera. In plastica coerenza tra diritto e tecnologia, la relativa operazione informatica è concretamente affidata ai server operanti presso i notariati di provenienza.
Resterà soggetta ovviamente ai comuni principi la soluzione della diversa questione della necessità della forma notarile per un determinato atto.

4.5 - *L'impiego della chiave privata da parte di soggetto diverso dal titolare*
Come si è osservato al §3, la firma digitale non garantisce l'identificazione dell'autore di una firma. Dall'esame della sottoscrizione, non è in alcun modo possibile determinare chi fisicamente l'abbia apposta: all'opposto di quanto accade nella firma tradizionale, tale circostanza può essere accertata solo basandosi su elementi esterni. Si possono distinguere due ipotesi principali [51], a seconda che il controllo del dispositivo di firma sia stato dal titolare rimesso volontariamente ad altri [52], oppure sottratto con frode o violenza; va inoltre considerata la possibilità che il certificatore abbia rimesso la chiave privata a soggetto diverso dal titolare.

4.5.1 - *L'affidamento volontario*
Affidare scientemente ad altra persona il proprio dispositivo di firma può essere empiricamente descritto, in prima approssimazione, come un fenomeno riconducibile alla rappresentanza [53]. Sussistono però differenze concettuali importanti, che ruotano intorno ad un rilievo fondamentale: la firma sarà per sua

---

statunitensi, la cui (per usare un eufemismo) non eccelsa affidabilità era perfettamente nota a tutti gli addetti ai lavori. Il veto di Obama è legato alla crisi del mercato ipotecario: circola negli Stati Uniti una tal massa di documenti ipotecari inaffidabili da far sembrare utile ogni barriera alla loro circolazione, anche all'interno degli USA. Per il contesto in cui si inquadra la vicenda si veda anche *Bank foreclosure cover seen in bill at Obama's desk*, servizio del 6 ottobre 2010 di S. J. PALTROW per Reuters, disponibile su www.reuters.com.

50 Si tratta del sistema descritto nell'articolo citato a nota 1, che assicura la circolazione degli atti notarili informatici all'interno dell'Europa. Il nome Bartolus (www.bartolus.eu), in onore del grande sassoferratese, è stato scelto dal notariato europeo, su proposta di chi scrive, in epoca successiva alla pubblicazione dell'articolo appena richiamato.

51 M. DOLZANI, *Il regime delle responsabilità. Obblighi dei soggetti interessati e spunti per un inquadramento sistematico*, in *Firme elettroniche. Questioni ed esperienze di diritto privato*, Studi del Consiglio Nazionale del Notariato, Giuffrè, Milano 2003, p. 65.

52 Sarà per lo più sufficiente consegnare dispositivo di firma e PIN.

53 L'accordo tra titolare ed effettivo utilizzatore del dispositivo possa essere espresso, e magari anche formalizzato per iscritto: nell'ipotesi che qui si presenta si assume però che tale accordo, se esistente (ed impregiudicata ogni considerazione sulla sua liceità: scettico nel sistema italiano M. DOLZANI, citato a nota 51), non sia esternato. Può naturalmente darsi l'ipotesi opposta: che Tizio, utilizzando la firma di Caio, renda palese (non nella firma, ma) nel corpo del documento, che è Tizio a firmare su incarico di Caio. Al di là dell'anomalia dell'impiego in un siffatto contesto della firma del rappresentato, si rientra qui con ogni verosimiglianza nell'orbita della rappresentazione, giacché se ne ha l'elemento più caratterizzante: la *contemplatio domini*.

intrinseca natura totalmente ed irreversibilmente indistinguibile da quella apposta dal titolare [54]. Il documento apparirà dunque, anche all'esame più accurato immaginabile, come proveniente direttamente dal titolare medesimo, e non si avrà alcuna *contemplatio domini*; il terzo non potrà in alcun modo apprezzare la fonte della rappresentanza (ammesso sempre che in questi termini si desideri parlare) né (ad esempio) i suoi limiti. Non a caso, l'ipotesi è stata spesso accostata al biancosegno [55], e sembra questa in effetti l'analogia più azzeccata per la ricerca di un'idonea soluzione sul piano internazionalprivatistico. Atteso che l'ipotesi in esame si colloca però interamente al di fuori del rapporto col certificatore, se ne desume che non vi sia spazio per un'applicazione, neppure parziale, della *lex attestationis*. Ciò sia detto con almeno due riserve. In primo luogo, in alcuni ordinamenti, e/o in relazione ad alcuni tipi di firma [56], la firma digitale non è suscettibile di alcun tipo di delega, ma ciò rileverà per lo più sul piano interno, quale violazione dei doveri [57] che incombono sul titolare, senza alcun influsso quindi sulla soluzione del problema qui proposto. In secondo luogo, mentre un biancosegno consente di produrre un solo documento, la consegna del dispositivo consente di produrre una serie infinita di documenti: se un argomento meramente quantitativo può reputarsi a giusto titolo irrilevante sul piano teorico, al § 4.5.3 si proporrà un angolo visuale parzialmente diverso.

4.5.2 - *La firma apocrifa*

La circostanza che una firma digitale sia stata apposta da un soggetto non autorizzato, è circostanza che può derivare da cause eterogenee [58] ed ha rilievo diverso nei vari ordinamenti [59]. Si tratta essenzialmente di un problema di prova,

---

54 A tre lustri quasi di distanza, appare sempre più lucido il suggerimento di M. MICCOLI (*Documento e commercio telematico*, IPSOA, Milano 1998, p. 35) di impiegare l'espressione *sigillo informatico* in luogo di *firma digitale*: come il sigillo, la firma digitale è indifferente all'autore materiale dell'operazione.

55 In argomento ZAGAMI, *op. cit.*, p. 289.

56 Come le firme/funzione di cui al §4.4.

57 Come l'obbligo di utilizzo personale del dispositivo sancito per il notaio italiano dal comma 3 dell'articolo 23ter della legge 16 febbraio 1913, n. 89 (inserito dall'articolo 1 del DLgs 2 luglio 2010, n.110).

58 Può darsi che venga sottratta la smart card unitamente al relativo PIN. Impadronirsi di quest'ultimo richiede tecniche di grado assai diverso di sofisticazione a seconda del livello d'attenzione del titolare: talvolta è sufficiente saper leggere (non sono rari i casi attestati di PIN trascritti su un Post-It conservato con la smart card) talaltra occorre installare fraudolentemente appositi keyloggers sul computer del titolare, o addirittura tentare l'intercettazione dei segnali elettrici emessi dalla tastiera. Può però anche accadere che la smart card sia consegnata dal certificatore a soggetto diverso dal titolare. Si veda *Ha la firma digitale, ma non lo sa...* http://www.interlex.it/docdigit/nonlosa.htm.

59 Per tacere poi delle evoluzioni che si sono registrate in vari ordinamenti, ed è probabilmente il nostro Paese a detenere il primato:

- 1997 (DPR 10/11/97 n. 513, GU 13/3/98 n. 60), articolo 5 comma 1: *Il documento informatico, sottoscritto con firma digitale ai sensi dell'art. 10, ha efficacia di scrittura privata ai sensi dell'art. 2702 del codice civile*;

materia che, come è ben noto, non offre in campo internazionale soluzioni stabili a causa dell'interferenza con la delicata ed incerta questione della natura sostanziale o processuale delle relative normative [60]. Ai limitati fini di queste considerazioni, basterà annotare che *prima facie* non parrebbe esservi neppure qui spazio per l'applicazione diretta della *lex attestationis,* almeno laddove l'anomalia non coinvolga il ruolo del certificatore, ad esempio qualora si assuma che l'apposizione di firma abbia avuto luogo sottraendo il dispositivo al controllo del titolare [61].
Qualora si ipotizzi invece che la chiave segreta sia sotto il controllo di terzi per comportamento imputabile al certificatore, l'analisi della disciplina che la *lex attestationis* detta per l'azione del certificatore assumerà rilievo, ma probabilmente solo sul piano della ricostruzione dei fatti [62].
Si veda però al paragrafo successivo.

4.5.3 - *Una considerazione sistemica*

Ancorché implementato con sfumature diverse, è ampiamente condiviso tra gli ordinamenti [63] il principio secondo cui chi sceglie un determinato mezzo di

---

- 2000 (DPR 28/12/00 n. 445, GU 20/2/01 n. 42), articolo 10 comma 1: *Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 e per le pubbliche amministrazioni, anche di quelle di cui all'articolo 9, comma 4, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile*;
- 2002 (DLgs 23/1/02 n. 10, GU 15/2/02 n. 39), 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*;
- 2005 (DLgs 7/3/05 n. 82, GU 16/5/05 n. 112), articolo 21 comma 2: *Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria*;
- 2010 (DLgs 30/12/10 n. 235, GU 10/1/11 n. 6), articolo 14 comma 1: *Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*.

La vista d'insieme lascia però cogliere un'evoluzione tutto sommato fruttuosa, con l'eccezione della sfortunata versione del 2002, che fu oggetto di un vero e proprio tiro al bersaglio (l'espressione è di P. RICCHIUTO, in *La "nuova" efficacia probatoria della firma digitale*, in Interlex 14/2/02, http://www.interlex.it/docdigit/ricchiu5.htm) cui si unirono anche M. MICCOLI e l'estensore di queste righe in *La forma sine probatione,* in *Notariato* (IPSOA), 2002, p. 329.

60 Si veda R. BARATTA, *Commento all'articolo 12 SIDIP*, in *Nuove Leggi Civili Commentate*, 1996, p. 1011.

61 La *lex attestationis* può però rilevare in relazione a profili collegati. Immaginiamo che il titolare, resosi conto di aver perso il controllo del dispositivo di firma, chieda al certificatore di provvedere alla revoca e questi non vi provveda nei tempi previsti dalla legge applicabile e/o dal rapporto contrattuale intercorrente tra titolare e certificatore.

62 Oltre che per la definizione della responsabilità del certificatore.

63 Si veda ad esempio The Commission on European Contract Law (Lando-Commission), *Principles of European Contract Law (parts 1 & 2)*, Kluwer Law International, The Hague 2000, p. 244.

comunicazione è chiamato a sopportare i rischi di una sua disfunzione. Adottare un sistema di firma digitale comporta rischi significativi, di svariato genere [64]. In prima approssimazione, sembra razionale affermare che chi impiega la firma digitale, avendo liberamente scelto tale sistema di documentazione, ne debba sopportare i rischi. Questo approccio suggerisce però almeno due ordini di considerazioni.

In primo luogo, l'argomento diviene sterile quando l'impiego della firma digitale è imposto dal destinatario [65], come accade in svariate applicazioni di e-Government.

In secondo luogo, il regime giuridico della firma digitale può essere uno degli elementi presi in considerazione da chi decide di dotarsi di un dispositivo di firma. Si prenda il più banale degli esempi: le tessere ATM, in Italia meglio note come Bancomat. Tali strumenti sono invariabilmente provvisti di limiti quantitativi e qualitativi di utilizzo: se così non fosse, dotarsene equivarrebbe ad assumere rischi che la maggior parte degli utenti giudicherebbe a giusta ragione inaccettabili. Qualunque delinquente di strada, estorto il PIN con una pistola puntata alla tempia del malcapitato titolare, potrebbe ripulirne per intero i risparmi. La possibilità di azioni criminali particolarmente lucrose attirerebbe poi nel "mercato" delinquenti più aggressivi ed organizzati, in una nefasta spirale.

Lo stesso tipo di analisi può applicarsi al nostro caso. Dotarsi di un dispositivo di firma capace di produrre documenti suscettibili di impegnare ogni ambito della sfera giuridica del titolare ed estremamente difficili da disconoscere, è scelta che comporta l'accettazione di un determinato livello di rischio. Qualora invece l'ordinamento del Paese di emissione (la *lex attestationis*, secondo la formula sopra proposta) riservi al titolare margini più ampi, od addirittura ponga sulla controparte l'onere della prova della genuinità della firma [66], l'adozione della firma digitale sarà opzione meno impegnativa, e coerentemente renderà plausibili comportamenti meno rigorosi sul fronte della sicurezza.

E' molto arduo immaginare che l'affidamento così riposto dal titolare nel regime giuridico della firma possa essere posto nel nulla qualora il documento sottoscritto sia soggetto ad una legislazione diversa dalla *lex attestationis,* circostanza che, in caso di uso fraudolento, è totalmente fuori dal controllo del titolare. Se si può perdonare il reiterato ricorso ad una metafora così dozzinale: difficile supporre che una carta ATM possa svuotare interamente il conto del titolare solo perché utilizzata presso uno sportello automatico sito in un Paese la cui legislazione (in

---

64 Ho avuto occasione di menzionarne alcuni in *Sicurezza tra mondo reale e virtuale*, comunicazione (http://xoomer.virgilio.it/ubechini/congr_naz_not_2004_bechini.htm) presentata il 3 dicembre 2004 al Congresso Nazionale del Notariato in Roma.

65 Così S. MASON, *op. cit.* , p. 311. A tale opinione M. NASTRI e chi scrive hanno già aderito nella relazione *Il notaio e la contrattazione elettronica*, presentata al XXIV Congresso Internazionale del Notariato Latino, Città del Messico 2004: p. 159 dell'edizione a stampa (Giuffrè, Milano 2004), a p. 37 della versione pdf disponibile sul sito www.notariato.it ed a p. 35 della versione in lingua spagnola, *El notario y la contración electrónica*, disponibile sul sito www.bechini.net.

66 Si veda a nota 25.

ipotesi) non preveda limiti di impiego.
Pare quindi di poter affermare che le regole della *lex attestationis* relative all'imputabilità del documento firmato al titolare del certificato, ed (in particolare) alla possibilità per il titolare stesso di procedere al disconoscimento, debbano essere comunque tenute in prudente considerazione, temperando le regole della legislazione ordinariamente applicabile, laddove queste ultime siano più vincolanti e rigorose per il titolare.

4.6 - *La forma*
L'idoneità del documento firmato digitalmente a soddisfare i requisiti di forma è questione che deve essere risolta secondo le norme dell'ordinamento applicabile secondo i comuni principi internazionalprivatistici. Si può riproporre qui il rilievo già presentato al § 4.2: non v'è apparente ragione per cui il giudizio di valore proprio di tale ordinamento debba cedere il passo a quello proprio dell'ordinamento di provenienza della firma stessa.
La legge italiana contiene (conformemente all'articolo 7 della direttiva 93/1999/CE) , espresse previsioni che equiparano alcune firme straniere a quelle italiane [67].

4.7 - *Manipolazioni del documento*
Allo stato attuale della tecnologia, non sembra verosimile [68] che il documento firmato digitalmente possa essere in alcun modo manipolato dopo la firma [69]. Un'eventuale allegazione di tal fatta [70] sarebbe comunque questione eminentemente probatoria, governata dall'ordinaria disciplina.

---

67 DLgs 82/05, articolo 21 comma 4. *Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:*
(a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;
(b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
(c) *il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali*.
DLgs 82/05, articolo 29 comma 8. *Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE e' equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo*.

68 Si veda a nota 20.

69 *Rectius*, tale manipolazione emergerebbe in sede di verifica delle firma, ed il fallimento della verifica priva la firma di ogni valore. Tale nozione fa parte del concetto stesso di firma digitale, e non pare suscettibile di trattamenti diversi nei vari ordinamenti.

70 Interessanti le considerazioni di S. MASON sulla *Presumpion of being in order* in *Electronic Evidence*, LexisNexis/Butterworths, London 2010, p. 109 ss.

5. ASSENZA DI ANALOGIE TRA CERTIFICAZIONE E RUOLO DEL NOTAIO

Nessuna somiglianza sussiste tra attività di certificazione digitale ed autentica notarile. Il certificato è lo strumento che consente di dare un senso alla firma digitale della parte, che altrimenti, come sopra già si è osservato, non ne avrebbe alcuno e resterebbe un'indecifrabile sequenza di caratteri. L'autentica notarile interviene invece a corroborare una firma che è già provvista di una sua autonoma valenza e riconoscibilità. Va ricordato [71], per di più, che il certificato ha ad oggetto la chiave pubblica e non il singolo documento, la cui stessa esistenza sarà di regola ignota al certificatore.

In caso di autentica notarile di una firma digitale [72], le parti firmeranno digitalmente sulla base dei propri certificati, e l'autentica stesa dal notaio sarà a sua volta firmata digitalmente sulla base del certificato del notaio [73]. Appare insomma chiaro come certificazione digitale ed attività del notaio si muovano su piani del tutto indipendenti [74].

Analoga la situazione in caso di atto pubblico [75], documento che promana essenzialmente dal notaio ed in cui la sottoscrizione delle parti svolge un ruolo concettualmente subordinato, tanto da poter persino mancare se la parte non può sottoscrivere [76]. In caso di atto pubblico digitale [77] l'atto sarà suggellato dalla firma digitale del notaio, emessa ovviamente sulla base del suo proprio certificato

---

71 Si veda *retro*, § 3.

72 Disciplinata in Italia sin dal 1997: DPR 10/11/97 n. 513, GU 13/3/98 n.60, articolo 16. La norma è stata poi trasfusa in tutti I testi successivi.

73 Supra, § 4.4.

74 Per una disamina, solo parzialmente suparata dalle recenti modifiche legislative, delle questioni giuridiche connesse alla produzione da parte del notaio di documenti digitali, si veda S. CHIBBARO, *Le problematiche giurdiche delle prime applicazioni*, in *Firme elettroniche. Questioni ed esperienze di diritto privato*, Studi del Consiglio Nazionale del Notariato, Giuffrè, Milano 2003, p. 101. L'Autrice ha pure curato lo Studio n. 2-2006/IG del Consiglio Nazionale del Notariato, *Codice dell'amministrazione digitale, firme elettroniche e attività notarile*, reperibile sul sito www.notariato.it. Di taglio più teorico l'indagine di E. A. GAETE GONZÁLES, *Instrumento público electrónico*, Bosch, Barcelona 2002.

75 Figura che nel panorama internazionale non è peraltro ovunque presente, almeno non nella versione “pura” nota in Italia e di cui al testo.

76 Articolo 51 della legge 16 febbraio 1913, n. 89.

77 Il primo atto notarile dematerializzato al mondo è stato ricevuto a Parigi il 28 ottobre 2008. Il Guardasigilli protempore, Rachida Dati, lo ha firmato con uno stilo su una tavoletta elettronica collegata ad un computer portatile, mentre il notaio rogante, Bernard Reynis di Parigi, ha chiuso l'atto con la sua firma digitale inoltrandolo seduta stante alla struttura centrale di conservazione dei notai francesi a Venelles, presso Aix-en-Provence. In Italia la figura, al giugno 2011, ha applicazione solo parziale, in mancanza di alcune integrazioni a livello regolamentare, ma è disciplinata dagli articoli 47bis, 47ter e 52bis della legge 16 febbraio 1913, n. 89 (inseriti dall'articolo 1 del DLgs 2 luglio 2010, n.110); la struttura di conservazione predisposta in Roma dal Consiglio Nazionale del Notariato è da parte sua già funzionante.

digitale.

Secondo quanto è dato a chi scrive prevedere, non è probabile però una diffusione in larga scala dell'autentica notarile della firma digitale (o dell'intervento in atto pubblico di privati muniti di firma digitale): assai più pratico appare il ricorso da parte del privato ad una semplice firma elettronica consistente nell'acquisizione elettronica della firma tradizionale degli interessati [78]. Il tema esula da queste brevi note, se non per il banale rilievo che l'atto è pur sempre conchiuso dall'abituale firma digitale del notaio.

6. TIMESTAMPING

Il timestamping, o validazione temporale [79], si sostanzia, in ultima analisi, in un'informazione firmata digitalmente: la certificazione dell'anteriorità di un file rispetto ad un certo momento. Si tratta dunque di un mezzo di prova, e come tale reputo vada trattato in prospettiva internazionale. Si dovrà in particolare apprezzare, volta per volta, se le modalità di rilascio del timestamping forniscano sufficienti garanzie nella prospettiva della legge applicabile. Si consideri ad esempio il caso della legislazione italiana, che da un lato attribuisce al timestamping uno status assimilabile a quello della data certa, ma dall'altra, coerentemente, ne regolamenta il rilascio in modo rigoroso [80]. Se non v'è ragione per negare aprioristicamente funzione di prova ad un timestamping emesso da soggetto che opera nell'ambito di altro ordinamento, se ne dovranno però soppesare le qualità intrinseche, con particolare riguardo per l'affidabilità tecnica e le garanzie di indipendenza del soggetto emittente, onde stabilire l'equiparabilità del timestamping straniero a quelli interni.

7. ESTENSIBILITA' DELLE CONCLUSIONI AD ALTRE FIGURE DI FIRMA ELETTRONICA

Le peculiarità che è parso di poter individuare nella firma digitale, capaci di influenzarne l'inquadramento internazionalprivatistico, hanno il proprio fulcro nello specifico ruolo del certificatore. Le conclusioni raggiunte possono quindi essere verosimilmente replicate a proposito di ogni figura di firma elettronica la cui rilevanza giuridica dipenda dal ruolo di un soggetto terzo. Le ordinarie firme

---

78 Questa è anche la prassi francese (si veda alla nota precedente) e statunitense: negli USA è anzi in vendita da anni un hardware specializzato, Enjoa (http://www.nationalnotary.org/enjoa/).

79 R. ZAGAMI, *op. cit.*, p. 209; FORD e BAUM, *op. cit.*, p. 355; CAMMARATA e MACCARONE, *op. cit.*, p. 138.

80 DLgs 7/3/05 n. 82, articolo 20.

elettroniche [81] resteranno invece soggette, se si condivide l'approccio che è stato qui proposto, alle comuni regole del diritto internazionale.

81 Ad esempio: cattura dell'immagine di una firma tradizionale, comuni messaggi di posta elettronica o SMS.