La firma elettronica
Lo stato dell'arte e le prospettive della standardizzazione in Europa

Il progresso tecnologico e l'adeguamento legislativo hanno profondamente innovato il panorama dell'autenticazione elettronica negli ultimi anni. Nel mondo di Internet succede infatti che sia la legge ad inseguire l'evoluzione della tecnologia e non viceversa.

E' opinione comune fra gli addetti ai lavori che l'infrastruttura a chiave pubblica che va creandosi possa ridurre drasticamente il costo delle transazioni in ogni settore di business, sia pubblico che privato. Pertanto, la riduzione dei costi fissi di transazione può comportare una trasformazione del modo di fare business.

Al fine di attribuire alla firma elettronica una piena rilevanza legale, l'obiettivo primario che le autorità di regolamentazione, in particolare quelle europee, si sono poste è stata la sicurezza delle comunicazioni e delle transazioni online, in particolare sotto l'aspetto dell'autenticazione e unicità del firmatario e dell'immodificabilità della comunicazione intercorsa.

Almeno tre sono gli approcci legislativi e regolamentari che sono stati scelti al fine di costituire il quadro legale idoneo a favorire la diffusione dell'uso della firma elettronica nei rispettivi ordinamenti giuridici:

1. L'approccio "minimalista" si è proposto di facilitare l'utilizzo delle firme elettroniche rimuovendo eventuali ostacoli di carattere legale al loro riconoscimento. Tale approccio è stato definito "bottom-up" nel senso che si lascia agli operatori del settore la possibilità di definire caratteristiche e modelli di sicurezza. L'espressione è corretta dal punto di vista degli operatori dei CSP. Ma dal punto di vista degli utilizzatori questi risulterebbero altrettanto calati dall'alto quanto le norme imposte dal legislatore (Canada, Stati Uniti, UK, Australia, Nuova Zelanda).

2. Un secondo approccio, "top-down", ha voluto essere più incisivo, fissando alcuni elementi imprescindibili per la validità della firma elettronica: adozione della crittografia asimmetrica, imposizione di requisiti operativi e finanziari per i CSP e di determinati doveri per i possessori di chiavi, delimitazione delle fattispecie e/o dei valori nei quali la firma elettronica è legalmente vincolante. Questo secondo tipo di approccio ha visto il legislatore e le autorità regolamentari dei rispettivi Paesi influenzare direttamente con le proprie norme la creazione della normazione di carattere tecnico e degli standards relativi a tali nuove tecnologie (prima legge tedesca e prima legge italiana, entrambe del 1997, Argentina, Malesia).

3. Il terzo approccio, adottato dall'Unione Europea, può essere considerato una sintesi dei due precedenti in quanto, se è pur vero che è importante consentire all'industria di autoregolamentarsi, è altrettanto certo che è imprescindibile fissare il quadro normativo di riferimento che garantisca il rispetto dei diritti delle persone nei confronti delle quali l'attività economica e tecnologica si esplica. Da una parte, l'Unione Europea impedisce agli Stati Membri di negare valore legale ad una firma solo perché è in forma elettronica o perché non soddisfa i requisiti di sicurezza previsti per la "firma elettronica avanzata". In tal senso ha un approccio minimalista al fenomeno della firma elettronica. Da un altro punto di vista, la direttiva europea richiede che per il pieno valore legale della "firma elettronica avanzata" quale firma autografa, essa debba essere creata mediante l'utilizzo di un SSCD e debba essere munita di un certificato qualificato (oltre all'Unione Europea, Singapore).

Il 19 luglio 2001 è scaduto il termine che l'Unione Europea aveva concesso agli Stati Membri per adeguare la propria normativa ai principi espressi dalla direttiva 1999/93/EC relativa ad un quadro comunitario per le firme elettroniche. Solo un ristretto numero di Stati membri ha pienamente recepito tali principi: in Italia il recepimento è avvenuto con il D.Lgs. 23 gennaio 2002 n. 10.

Il ritardo di buona parte degli Stati Membri nel recepire i principi espressi nella direttiva non può essere spiegato soltanto mediante la lentezza dei procedimenti legislativi e burocratici o essere dovuto solo ad una insufficiente volontà politica. In realtà, il fatto che la normativa comunitaria esprima uno schema di legislazione caratterizzato dalla "co-regolamentazione", e cioè dal concorso degli standards internazionalmente riconosciuti nel definire lo specifico contenuto dei precetti espressi dalla direttiva, ha fatto sì che più di uno Stato membro abbia atteso o stia attendendo l'esito del processo di standardizzazione avviato nell'ambito dell'EESSI, di cui si dirà appresso, al fine di definire in modo concreto ed operativo il quadro legale di riferimento per la firma elettronica.

Infatti, la direttiva 1999/93/EC si è limitata a sancire i principi del libero accesso al mercato, della non discriminatorietà della normativa di settore, della necessità di un'adeguata tutela dei dati personali, della necessità di un'adeguata responsabilità dei prestatori dei servizi di certificazione, della necessità di un adeguato sistema di supervisione e di un'adeguata tutela del consumatore.

Ma la Comunità ha demandato all'industria e agli enti di standardizzazione nazionali, nel quadro di riferimento costituito dall'ICTSB, di analizzare la necessità e le modalità di standards operativi che supportino tecnicamente il quadro legislativo delineato dalla direttiva, così da favorire uno sviluppo coerente e significativo dei prodotti e dei servizi di firma elettronica. La partecipazione di pubblico e privato sembra aver garantito il giusto equilibrio tra esigenze politiche e di mercato.

Nel 1999 è stata quindi lanciata l'iniziativa EESSI, condotta in stretta collaborazione da due enti costituenti l'ICTSB: il Cen/Isss e l'Etsi.

Il lavoro svolto in questi anni dai gruppi di lavoro Ws E-Sign (nell'ambito di Cen/Isss) e Sec Esi (nell'ambito di ETSI) ha portato alla redazione di documenti che hanno la configurazione di "pre-standards": si tratta di norme tecniche che non hanno un loro status ufficiale e non possono dunque essere oggetto di riferimenti nell'ambito di leggi o regolamenti statali, ma che possono essere di estrema importanza economica e tecnica. Basti pensare che il GSM è una norma tecnica, un "pre-standard", elaborato da ETSI. Al fine di divenire standard nazionali, europei o mondiali, i pre-standards debbono essere assoggettati alla procedura formale di approvazione dei rispettivi enti ufficiali di standardizzazione nazionali (UNI, DIN, BS, etc.), europei (Cen o ETSI), oppure internazionali (ISO).

In seguito alle dichiarazioni del commissario Liikanen alla EESSI Conference di Bruxelles del 19 giugno 2001, è da ritenersi estremamente probabile che il Comitato previsto dall'art. 9 della Direttiva 1999/93/EC referenzi detti standards e ne raccomandi alla Commissione la loro pubblicazione nella Gazzetta Ufficiale delle Comunità Europee. Tale comitato non è un ulteriore ente di standardizzazione, bensì un organo di consulenza tecnica composto da rappresentanti ufficiali di tutti gli stati membri dell'UE, che ha la funzione di supportare il processo di recepimento degli standards internazionali nell'ambito della normativa comunitaria in materia di firma elettronica.

Il recepimento in toto di norme tecniche e standards nella normativa comunitaria costituisce la principale innovazione delle c.d. direttive di nuovo approccio, che realizzano in tal modo una forma di concorso fra normativa dettata dal legislatore e autoregolamentazione, battezzata con un neologismo: "co-regolamentazione", in inglese "co-regulation".

Vediamo più nel dettaglio quali sono stati gli aspetti standardizzati.

Nell'ambito di Etsi Sec Esi, i formati della firma (ETSI TS 101 733); i requisiti per i CSP (ETSI TS 101 456) e per le TSA (ETSI TS 102 023), i profili dei certificati qualificati (ETSI TS 101 862) e della marcatura temporale (ETSI TS 101 861). Inoltre, la gestione e le linee di condotta dei CSP per quanto riguarda i certificati non qualificati (ETSI TS protocollo ancora non definito), la firma elettronica avanzata in ambiente XML (ETSI TS 101 903), le linee di condotta per la firma elettronica (ETSI TR 102 038).

Nell'ambito del Cen/Isss Ws E-Sign, sono stati determinati i requisiti di sicurezza per i *Trustworthy Systems* che gestiscono i certificati (CWA 14167-1), i requisiti di sicurezza dei SSCD (CWA 14168 e 14169) e le linee guida per la loro implementazione (CWA 14255), i requisiti di sicurezza degli ambienti e delle procedure per la creazione (CWA 14170) e la verifica della firma (CWA 14171), i moduli crittografici per i CSP (CWA 14167-2), oltre a una guida per l'accertamento della conformità, molto importante per la definizione dei ruoli dei sistemi di accreditamento (CWA 14172).

Cen/Isss Ws E-Sign sta tuttora lavorando su altri importanti temi, quali l'uso sicuro dei certificati in ambienti specifici (ad esempio le applicazioni per l'e-commerce) e

l'interoperabilità delle smartcards. A sua volta, Etsi Esi Wg si pone obiettivi ambiziosi per quanto riguarda l'armonizzazione dei servizi di certificazione.

Per garantire la consistenza dell'attività svolta in EESSI è stato affidato a sei esperti "esterni" di fama internazionale, il compito di valutarne la conformità ai principi della direttiva europea.

Poiché è già stata realizzata una notevole mole di lavoro, i lavori di EESSI potrebbero terminare fra la fine del 2002 e l'inizio del 2003.

A tutt'oggi la partecipazione dell'industria italiana ai lavori è stata scarsa, ma la speranza è che i certificatori italiani, i produttori di smartcards, i produttori di software e dispositivi di firma abbiano seguito da lontano ma con attenzione il processo di standardizzazione, per non ritrovarsi un domani a dover riposizionare o riconfigurare in modo significativo i propri prodotti/servizi.

Il processo di adeguamento dell'Italia alla Direttiva 1999/93/EC è invece giunto a termine. Con il decreto legislativo 23 gennaio 2002 n. 10, l'Italia ha pienamente recepito i principi della direttiva relativa ad un quadro comunitario per le firme elettroniche.

Alcuni spunti di riflessione.

Il testo pubblicato in G.U. introduce alcune importanti novità al T.U. 445/2000.

In primo luogo, il decreto legislativo attribuisce valore probatorio al documento sottoscritto con firma elettronica "leggera" (Art. 6 c. 2: "*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.*").

Questa previsione va probabilmente al di là della previsione comunitaria, il cui unico obiettivo è impedire che ad un documento con firma "non sicura" sia negato a priori un valore probatorio. Il fatto che sul piano probatorio il documento sia liberamente valutabile può essere inteso nello stesso senso in cui si valuterebbe, in caso di incertezza, se un documento cartaceo sia stato scritto con caratteri indelebili o a matita. Si tratta di una innovazione coraggiosa di cui è difficile prevedere gli esiti pratici.

Per evitare il proliferare di contenzioso in materia di firma elettronica "leggera", è molto importante che nella sua implementazione si tenga conto dei più recenti standards in via di elaborazione da parte di EESSI e di alcuni importanti progetti di ricerca in materia, finanziati dall'Unione Europea ed in corso di pubblicazione.

È addirittura inquietante che con riferimento alla firma elettronica "pesante" si sia giunti ad affermare che il documento informatico, quando è sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata generata mediante un SSCD, e connessa ad un certificato qualificato, "*fa piena prova fino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritto*" (Art. 6 c. 3). A parte il difetto di coordinamento con gli articoli 2702 e 2703 del Codice Civile, di fatto si attribuirebbe al

certificatore un ruolo sostanzialmente equivalente a quello del Pubblico Ufficiale. Ma è lecito chiedersi se con la stessa affidabilità e autorevolezza. Infatti:

1) Il processo di identificazione per il rilascio di uno strumento di firma digitale oggettivamente non offre le stesse garanzie della identificazione effettuata da un Pubblico Ufficiale (e ciò non solo perché il Pubblico Ufficiale risponde penalmente persino in caso di errore scusabile, a differenza dei certificatori);

2) La tecnologia non consente oggi di essere sicuri al 100% di firmare effettivamente il medesimo documento visualizzato sul display del computer o che è stato stampato. Il Pubblico Ufficiale garantisce proprio questo, persino nell'autentica di firma (e dunque non solo nell'atto pubblico);

3) Una scrittura privata o un atto pubblico sono atti che sono stati conclusi alla presenza di un soggetto terzo non interessato all'atto (il Pubblico Ufficiale), mentre i documenti firmati con la firma "pesante" non necessariamente sono redatti o sottoscritti alla presenza di un soggetto terzo e imparziale.

Ultima notazione: nella nuova normativa si introduce ex novo la "Carta Nazionale dei Servizi", che affiancherà la Carta d'Identità Elettronica e potrà essere utilizzata ai fini dei pagamenti tra soggetti privati e pubbliche amministrazioni. La decisione di separare la C.I.E dalla C.N.S è improntata ad un condivisibile pragmatismo. Probabilmente non sono maturi i tempi per fondere in un unico strumento due funzionalità entrambe complesse ma con caratteristiche di sicurezza significativamente diverse.

Queste innovazioni, proprio per l'essere così ardite, sollevano purtroppo dubbi di costituzionalità, per eccesso di delega (art. 2 lett. b).

Il Governo, delegato dalla L. 29 dicembre 2000 n. 422, c.d. Legge comunitaria, può infatti utilizzare il contenuto di una direttiva europea come criterio guida, introducendo modifiche o integrazioni alle discipline interessate dalla direttiva per evitare disarmonie con le discipline vigenti. La delega non è però così estesa da consentire al legislatore delegato di cambiare il sistema al di là di ciò che sia richiesto per il recepimento della direttiva.

Al di là di questi problemi formali, è possibile rilevare che probabilmente non si è tenuto sufficientemente conto dello stato della tecnologia e degli standards in materia: una loro più attenta considerazione avrebbe reso evidente che i tempi non sono maturi per un'equiparazione della firma elettronica alla scrittura privata autenticata.

Tuttavia sia in Europa che negli Stati Uniti si sta lavorando a tecnologie molto interessanti che possono addirittura rendere possibile la redazione a più mani di un atto digitale che può avere il medesimo valore probatorio di un atto pubblico.

Si tratta però di tecnologie che ancora non trovano una applicazione commerciale.

Dott. Riccardo Genghini (Notaio – Presidente di Cen/Isss Ws E-Sign)

Dott.ssa Daniela Rocca (Consulente Legale)

Studio Notarile Genghini – www.sng.it

Glossario	
CEN/ISSS	European Committee for Standardisation/Information Society Standardisation System
C.I.E.	Carta d'Identità Elettronica
C.N.S.	Carta Nazionale dei Servizi
CWA	Cen Workshop Agreement
CSP	Certification Service Provider
EESSI	European Electronic Signature Standardisation Initiative
ETSI	European Telecommunication Standards Institute
ICTSB	Information and Communications Technologies Standards Board
PKI	Public Key Infrastructure
SSCD	Secure Signature Creation Device
SEC ESI	Security – Electronic Signatures and Infrastructures
TR	Technical Report
TS	Technical Specification
WS E-SIGN	Workshop on Electronic Signatures