# Informatica e diritto

*Rivista internazionale*
dell'Istituto di Teoria e Tecniche
dell'Informazione Giuridica del CNR
*diretta da* Costantino Ciampi

## Il processo telematico



Edizioni Scientifiche Italiane

# La firma elettronica, garanzia tecnica e giuridica di sicurezza nel commercio elettronico

BERTIL COTTIER, SILVANO MARIONI*

SOMMARIO: *1. Introduzione – 2. L'importanza della chiave segreta – 3. Il problema della distribuzione delle chiavi – 4. La crittografia a chiave pubblica – 5. La firma digitale – 6. La necessità di soluzioni pratiche – 7. La fiducia nella chiave pubblica – 8. Le autorità di certificazione – 9. Il quadro normativo europeo – 10. La legislazione svizzera in tema di firma elettronica – 10.1. Le fonti legislative – 10.2. Il processo telematico*

## 1. INTRODUZIONE

Il successo del commercio elettronico si basa su due imperativi: il primo è tecnico, l'altro è giuridico.

Da un punto di vista tecnico bisogna assicurarsi che le transazioni siano confidenziali e sicure, o detto in altri termini che non possano essere ne intercettate ne modificate. Dal punto di vista giuridico deve essere messo in atto un quadro legislativo che, da una parte dia un valore legale ai documenti elettronici, e dall'altra assicuri che l'infrastruttura necessaria alle transazioni elettroniche sia di alta qualità e garantisca una sicurezza di primordine.

Senza queste condizioni il commercio elettronico non sarà mai affidabile (e in tutti i casi non sarà percepito come tale) e gli attori della vita economica, in primo luogo i consumatori, lo rifiuterebbero.

Per offrire il massimo della sicurezza e dell'affidabilità gli informatici hanno sviluppato uno strumento essenziale: la firma elettronica. Il presente contributo si concentrerà con una visione sia tecnica che giuridica su questo strumento decisivo, che non è tanto una firma nel senso classico del termine ma piuttosto un dispositivo tecnico di autenticazione e di protezione del testo digitale.

* Il presente lavoro nasce da una collaborazione degli autori sul tema delle relazione tra gli aspetti tecnologici e giuridici consolidatasi nell'organizzazione del Simposio "Tecnologia e Diritto" che si svolge ormai da nove anni a Bellinzona (http://www.ssig.ch/td). Bertil Cottier, professore ordinario di diritto della comunicazione presso la Facoltà di Scienze della comunicazione dell'Università della Svizzera italiana e professore associato di diritto dei nuovi media presso la Facoltà di diritto dell'Università di Losanna. Silvano Marioni, CISSP, responsabile e docente del Certificate of Advanced Studies Sicurezza Informatica presso la Scuola Universitaria Professionale della Svizzera Italiana. Consulente nei settori delle architetture Internet e della sicurezza informatica.

Nella prima parte, l'accento sarà messo sugli aspetti tecnici del funzionamento della firma digitale che è strettamente legato alla crittografia e in particolare alla crittografia a chiave pubblica. Per capire quale legame intercorre tra la crittografia e la firma digitale verrà ripercorsa la storia della tecnologia analizzando l'evoluzione delle esigenze e delle soluzioni di crittografia. La parte giuridica di questo articolo presenterà innanzitutto il diritto europeo sulla firma elettronica, per concentrarsi in seguito sulle soluzioni adottate dal legislatore svizzero. Quest'ultimo si è ispirato in modo autonomo al diritto europeo per adottare un quadro legislativo esaustivo e originale che va dall'equivalenza tra la firma elettronica e la firma autografa alle condizioni di riconoscimento delle chiavi di firma passando dalla responsabilità dei fornitori dei servizi di certificazione. Con l'obiettivo di promuovere lo sviluppo del commercio elettronico non solo a favore degli operatori svizzeri ma anche degli operatori stranieri.

## 2. L'importanza della chiave segreta

Un sistema crittografico permette di trasmettere in modo sicuro un messaggio tra due interlocutori che utilizzano una chiave di cifratura comune e segreta. Possiamo ricordare ad esempio il sistema di crittografia utilizzato da Giulio Cesare per comunicare con le sue legioni oppure i sistemi di crittografia, basati sui lavori di Leon Battista Alberti, Johannes Trithemius e Blaise de Vigenère, usati dagli stati nazionali nel rinascimento[1].

La condizione fondamentale per una comunicazione sicura è che lo scambio della chiave di cifratura avvenga tra gli interlocutori senza che terze persone riescano ad intercettarla. E questa è sicuramente una condizione che gli stati nazionali sono sempre stati in grado di garantire finché si trattava di comunicare con un numero relativamente limitato di emissari e ambasciatori.

La situazione diventa più complessa quando c'è la necessità di comunicare in modo cifrato con un numero sempre più grande di interlocutori, come ad esempio nelle comunicazioni militari; una distribuzione di massa delle chiavi segrete, con i conseguenti rischi di intercettazione, può creare non pochi problemi organizzativi.

[1] Vedi D. Kahan, *The Codebreakers*, New York, Scribner, 1996.

Nel corso dell'ultimo conflitto mondiale questo problema si manifestò chiaramente nei sistemi di crittografia utilizzati dagli eserciti di tutte le parti belligeranti. Un esempio tipico è il caso del sistema di crittografia utilizzato dall'esercito tedesco, la famosa macchina Enigma, un'apparecchiatura a batteria che era utilizzata per le comunicazioni sul campo di battaglia.

Enigma era dotata di una tastiera, una serie di lampadine corrispondenti alle lettere dall'alfabeto e un sistema di rulli mobili che modificavano, battuta dopo battuta, i collegamenti tra i tasti e le lampadine. Impostando una posizione iniziale dei rulli, il testo battuto sulla tastiera veniva cifrato diventando incomprensibile.

La controparte impostava la medesima posizione iniziale dei rulli e, ribattendo il testo cifrato, lo riotteneva leggibile; la posizione iniziale dei rulli era la chiave segreta di cifratura. Tutte le postazioni dotate di una macchina Enigma ricevevano regolarmente un identico libretto con le chiavi segrete che dovevano essere cambiate ogni giorno.

Questa condivisione della medesima chiave da parte di tutti gli interlocutori era la parte più debole del sistema perché dava agli avversari l'enorme vantaggio di poter analizzare un numero elevato di messaggi cifrati con la medesima chiave segreta. Aumentava in questo modo il rischio di scoperta della chiave segreta, caso in cui le comunicazioni di tutti gli interlocutori perdevano la loro segretezza

Questo fatto fu abilmente sfruttato dai servizi inglesi, che nel centro di Bletchley Park, riuscirono dopo molte prove a trovare il sistema per scoprire le chiave segrete e conseguentemente leggere i messaggi cifrati dell'esercito tedesco.

Una possibile soluzione poteva essere quella di avere una chiave segreta per ogni coppia di interlocutori ma questo avrebbe aumentato in modo esponenziale il numero delle chiavi segrete da distribuire con enormi problemi logistici.

## 3. Il problema della distribuzione delle chiavi

Il problema della distribuzione di massa delle chiavi segrete restò insoluto fino al dopoguerra, quando l'avvento dell'informatica avrebbe dato agli studiosi di crittografia nuove opportunità di ricerca e nuovi strumenti di lavoro.

I tempi stavano maturando e si stava preparando una vera e propria rivoluzione che avrebbe portato negli anni Settanta a sistemi di crittografia utilizzabili in contemporanea da più utenti.

Due ricercatori americani, Withfield Diffie e Martin Hellman, intuirono che nell'allora nascente rete Internet ci sarebbero state delle esigenze di riservatezza non solo per gli stati e le aziende, ma anche per le comunicazioni dei privati cittadini; per questo si doveva trovare una soluzione crittografica per condividere le chiavi segrete tra più interlocutori in modo indipendente, sicuro e semplice da usare.

Nel 1976 presentarono un sistema per lo scambio delle chiavi segrete attraverso l'invio di informazioni pubbliche. Il sistema prevedeva che gli interlocutori, dotati del medesimo algoritmo informatico, ottenessero ciascuno un numero che poteva essere scambiato pubblicamente e che reinserito dalla controparte nel medesimo algoritmo informatico generavano quasi miracolosamente un numero identico per entrambi: la chiave segreta.

Il sistema rivoluzionava i dogmi della crittografia ufficiale e permetteva la comunicazione con un numero infinito di interlocutori senza che si fosse precedentemente stabilito alcuno scambio di informazioni.

C'era solo un piccolo problema: i due interlocutori dovevano scambiarsi in contemporanea le informazioni e quindi il sistema non si prestava per comunicazioni differite nel tempo come ad esempio la posta elettronica.

### 4. La crittografia a chiave pubblica

La svolta fondamentale avvenne l'anno successivo quando tre ricercatori del MIT, Ronald Rivest, Adi Shamir e Leonard Adleman, stimolati dalle ricerche di Diffie e Hellman, intuirono la possibilità di un sistema di crittografia asimmetrico, in cui per cifrare e decifrare venivano utilizzati sistemi di calcolo e chiavi differenti.

Il sistema oltre a permettere lo scambio delle chiavi senza che gli interlocutori si conoscessero in anticipo, aveva il vantaggio, rispetto a quello di Diffie e Hellman, di poter essere utilizzato in modo differito; cosa che avrebbe permesso in seguito lo sviluppo dei sistemi di comunicazione sicura di Internet, dalla posta elettronica sicura al commercio elettronico.

L'algoritmo, che si chiamò RSA dalle iniziali dei suoi inventori, fu una grande rivoluzione rispetto alle tecniche della crittografia esistenti che prevedevano solo strumenti di cifratura in cui, sia il sistema di calcolo, sia la chiave segreta dovevano essere identici e simmetrici per i due interlocutori.

L'algoritmo RSA viene detto asimmetrico perché si basa su una coppia di chiavi complementari: una chiave, utilizzata per cifrare, che deve essere obbligatoriamente resa pubblica e una chiave utilizzata per decifrare, che deve essere mantenuta segreta.

Per inviare un messaggio protetto a qualcuno, basta ottenere la sua chiave pubblica e utilizzarla per cifrare, sicuri che il destinatario sarà in grado di decifrarlo con la sua chiave privata. In questo modo la crittografia a chiave pubblica garantisce una comunicazione riservata dei dati senza nessuno scambio anticipato di delle chiavi segrete.

Ma il grosso vantaggio che questo algoritmo asimmetrico aveva rispetto ai tradizionali algoritmi simmetrici è una funzione che fino ad allora non era neanche stata immaginata: la possibilità di avere la certezza che il messaggio era stato inviato da una persona definita e la garanzia che non fosse stato modificato.

## 5. La firma digitale

In questo caso le chiavi sono utilizzate in modo inverso. Il mittente cifra con la sua chiave privata e invia il documento al destinatario che se riesce a decifrarlo con la chiave pubblica del mittente ha la certezza della provenienza e dell'integrità del messaggio senza nessuno scambio preventivo di chiavi segrete. Queste sono le caratteristiche tipiche di un documento cartaceo a cui è stata apposta una firma autografa; da qui il nome firma digitale.

La tecnica della firma digitale ha una maggior robustezza rispetto alla firma autografa perché ogni tentativo di spostare la firma da un documento a un altro o di fare delle modifiche al testo viene immediatamente reso evidente[2].

Sia nel caso della crittografia che della firma digitale la chiave pubblica ha particolare importanza nell'identificazione della controparte. Nel primo caso essa garantisce l'invio di un messaggio protetto ad una persona definita, nel secondo caso permette di avere la certezza che il messaggio proviene da una persona definita.

[2] Per un approfondimento della firma digitale vedi American Bar Association, *Digital Signature Tutorial*, in http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html.

La certezza che la chiave pubblica appartenga veramente al titolare, che la dichiara come sua, diventa quindi il cardine di tutto il sistema, requisito fondamentale per evitare che un impostore possa utilizzarla per compiere attività fraudolente.

Prima di esaminare come può essere gestita la chiave pubblica, per completezza dell'esposizione conviene accennare brevemente alle soluzioni tecniche utilizzate per il funzionamento pratico del sistema.

### 6. La necessità di soluzioni pratiche

L'algoritmo RSA si basa sulla matematica dei grandi numeri e richiede una notevole potenza di calcolo. Per un documento di una certa dimensione i tempi di cifratura, trascurabili su un supercomputer accademico, possono diventare inaccettabili anche su un personal computer di ultima generazione. Per questo si sono dovute trovare delle soluzioni per ridurre le necessità di potenza di calcolo.

Nel caso della cifratura si utilizza un sistema ibrido; il documento – di qualsiasi dimensione – viene cifrato con un algoritmo simmetrico, molto veloce anche su computer poco potenti. Solo la chiave di cifratura simmetrica, lunga qualche decina di caratteri, viene quindi cifrata con l'algoritmo RSA usando la chiave pubblica del destinatario. Per decifrare si applica il processo inverso, decifrando la chiave simmetrica con la chiave privata del destinatario, e utilizzandola per decifrare il documento.

Analogamente anche per la firma digitale si utilizza un processo a due passaggi. In questo caso si utilizzano dei particolari algoritmi in grado di calcolare un riassunto del documento (*message digest*). La caratteristica di questi algoritmi (algoritmi di *hash*, ad esempio SHA e MD5) è quella di riassumere documenti di qualsiasi dimensioni in un testo di poche decine di caratteri. La modifica di un solo carattere del documento crea un riassunto completamente differente.

Date queste premesse tecniche, per firmare un documento si calcola il riassunto che viene cifrato con la chiave privata del mittente; i destinatari[3], ricevuto il testo e il riassunto cifrato, non devono far altro che decifrare il riassunto con la chiave pubblica del mittente e ricalcolare il

[3] Un documento firmato può essere naturalmente inviato a più destinatari.

riassunto del documento ricevuto. Se i due riassunti coincidono c'è la certezza che il documento proviene dal titolare della chiave pubblica e che non è stato alterato.

Tutto questo avviene in modo trasparente per l'utente che deve solo ricuperare le chiavi pubbliche delle controparti e fornire una *password* per liberare la sua chiave privata.

## 7. La fiducia nella chiave pubblica

Ma prima di affrontare il tema della chiave pubblica torniamo al nostro percorso storico per capire quali altri avvenimenti hanno caratterizzato la diffusione di questa tecnologia.

Nell'agosto 1977 viene pubblicato sulla rivista *Scientific American* una descrizione del nuovo algoritmo di cifratura RSA. A causa del ridotto spazio redazionale si invitano i lettori a richiedere direttamente a Ronald Rivest il documento completo con le spiegazioni dell'algoritmo. Contro ogni aspettativa questo documento venne richiesto da oltre 3.000 persone.

Tra di loro c'è Phil Zimmermann, un informatico preoccupato dell'ingerenza del governo nella vita privata dei cittadini, che decide di utilizzare l'algoritmo RSA per creare un programma di pubblico dominio per la cifratura dei dati personali.

Nel 1991 pubblica casualmente il suo programma Pretty Good Privacy[4] su Internet e questo gli causa una serie di problemi legali con l'azienda che aveva brevettato l'algoritmo RSA e con il governo americano. Ma il programma PGP si diffuse in tutto il mondo, diventando in breve un riferimento per la cifratura e la firma digitale dei documenti e contribuendo anche alla promozione dei successivi prodotti commerciali.

Uno dei motivi che ha contribuito alla diffusione di PGP, oltre al fatto di essere un programma gratuito, è la modalità con cui vengono considerate affidabili le chiavi pubbliche.

In PGP[5] la fiducia nelle chiavi pubbliche deriva o da una conoscenza diretta del proprietario della chiave o dal fatto che qualcuno di nostra

[4] Vedi S. Garfinkel, *PGP Encryption for everyone*, Cambridge, USA, O'Reilly, 1995.

[5] Vedi http://www.pgpi.org.

fiducia garantisce per lui. Queste informazioni possono essere verificata su appositi *server* (PGP *Public Key Server*) che però sono solo degli elenchi di chiavi associate ai nomi degli utenti e che, per la natura stessa del sistema, non sono in grado di dare nessuna informazione sull'affidabilità della chiave pubblica. La fiducia della chiave pubblica è una scelta personale del singolo utente e questa è stata una delle caratteristiche che ha permesso a PGP di svilupparsi in modo rapido fino a raggiungere l'attuale diffusione ma è anche il suo limite poiché non riesce a fornire un'informazione oggettiva sulla validità della chiave pubblica.

## 8. Le autorità di certificazione

Nei primi anni Novanta le esigenze di comunicazione sicura per il nascente commercio elettronico su Internet riaccendono l'interesse per la crittografia a chiave pubblica ma soprattutto sulla necessità di certificare in modo sicuro l'identità elettronica di un soggetto.

L'acquirente che decideva di acquistare il libro nel sito di Amazon.com voleva avere la certezza di consultare veramente il sito in questione e non quello di un impostore e pretendeva che i dati relativi al suo acquisto, in particolare il numero della carta di credito, fossero protetti dalla vista di estranei. La crittografia a chiave pubblica e la firma digitale fornivano la soluzione a entrambi i problemi ma bisognava assicurare che la chiave pubblica di un soggetto fosse veramente associata alla sua identità.

A questo scopo, in quegli anni, sorsero le prime società che si assumevano il compito tecnico, ed entro certi limiti legale, di certificare che una particolare chiave pubblica apparteneva veramente ad un soggetto definito. Erano nate le prime Autorità di Certificazione commerciali tra cui figuravano allora Verisign (oggi *leader* mondiale del settore), Entrust, Thawte, Baltimore, ecc.

L'Autorità di Certificazione è un organismo che – analogamente a un notaio – garantisce l'associazione tra un titolare e la sua chiave pubblica, tramite l'emissione di un Certificato Digitale.

La validità del Certificato Digitale è dato dal fatto che l'Autorità di Certificazione firma in modo digitale il certificato garantendo la sua integrità e si assume quindi la responsabilità della sua identificazione.

Il lavoro di una Autorità di Certificazione comprende una serie di attività quali l'identificazione dei soggetti, la generazione delle chiavi, la loro

distribuzione, la messa a disposizione del Certificato Digitale, il suo rinnovo alla scadenza, l'eventuale revoca in caso di perdita o di furto.

L'Autorità di Certificazione può gestire un gruppo chiuso di utenti (ad esempio all'interno di un'azienda) e in questo caso non si pongono particolari problemi legali o tecnici sulla gestione e l'utilizzo dei certificati poiché l'uso è limitato e disciplinato privatamente all'interno di un'organizzazione.

Nel caso di un'Autorità di Certificazione commerciale che offre i propri servizi al pubblico (ad esempio tutte le Autorità di Certificazione che garantiscono i siti di commercio elettronico) è importante che le attività siano disciplinate da un regolamento che dà ai clienti la certezza che le attività si svolgono in modo corretto. Questo regolamento, il *Certification Practice Statement*[6], disciplina sia le attività di fornitura dei Certificati Digitali nei confronti dei clienti, sia i processi di gestione interni all'Autorità di Certificazione.

È in questo contesto che si iniziò a parlare della necessità di dare valore legale alla firma elettronica[7], ma apparve subito evidente che l'efficacia e la validità della soluzione sarebbero state direttamente proporzionale al livello di condivisione tra gli attori delle diverse realtà nazionali. È in questo contesto che il modello legislativo europeo, proposto alla fine degli anni Novanta, ha acquistato un significato particolare.

## 9. Il quadro normativo europeo

Il diritto europeo sulla firma elettronica è fondato su un testo di base adottato nel 1999, la direttiva del 13 dicembre 1999 relativa al quadro comunitario per le firme elettroniche[8]. Questo testo intende definire un quadro giuridico chiaro e indispensabile allo sviluppo del commercio elettronico nello spazio del mercato interno. Il preambolo, alla sua cifra 4, sottolinea in effetti che "la divergenza delle norme in materia di rico-

[6] Vedi, ad esempio, il *Certification Practice Statement di Verisign* http://www.verisign.com/repository/CPS/VeriSignCPSv3.5.pdf.

[7] Il primo esempio di legislazione sulla firma digitale è stato lo *Utah Digital Signature Act* nel 1995.

[8] Vedi http://www.interlex.it/testi/99_93ce.htm.

noscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico".

Nei primi documenti legislativi si è sempre parlato di firma digitale fino a quando la l'Unione Europea ha deciso di disciplinare il settore con la direttiva 1999/93/CE in cui compare il termine firma elettronica. Volendo fare una precisazione tecnico-linguistica si deve dire che una firma digitale è un tipo particolare di firma elettronica che permette di identificare chi ha firmato un documento e contemporaneamente assicurare che il documento non è stato alterato, mediante l'utilizzo di un algoritmo matematico a tutt'oggi impossibile da falsificare.

L'obiettivo principale della direttiva è di assimilare la firma elettronica alla firma autografa, in modo da darle il valore di prova davanti a un tribunale (art. 5). Per contro la direttiva si rifiuta di armonizzare la regole nazionali sulla forma del contratto, in particolar modo la necessità della forma scritta; in effetti queste disposizioni sono molto differenti da un paese all'altro (basta guardare ai paesi anglosassoni che riconoscono raramente gli impegni in forma orale). Un'armonizzazione così estesa oltre a ritardare i lavori di adozione della direttiva, non sarebbe stata per nulla necessaria per assicurare il successo del commercio elettronico; quello che importa in effetti è di dare alla firma elettronica l'efficacia giuridica. In più è necessario che tutto questo offra un livello molto alto di sicurezza. A questo riguardo è importante sottolineare che la direttiva distingue tre tipi di firma elettronica a seconda del loro grado di sicurezza: si parla di firma elettronica semplice, firma elettronica avanzata e firma elettronica qualificata (art. 2). Anche se niente si oppone all'utilizzo delle due prime categorie di firma, la direttiva riconosce la piena validità giuridica solo alla firma elettronica *qualificata*.

La firma elettronica semplice riguarda dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione. La firma elettronica semplice può includere l'immagine digitalizzata di una firma autografa o una firma (ad esempio il testo Mario Rossi) alla fine di un documento elettronico. Non è basata su un certificato e non da nessuna indicazione sulla provenienza o l'autenticità della firma, limitando notevolmente il suo valore probatorio.

La firma elettronica avanzata è una firma elettronica che deve essere connessa in maniera unica e essere idonea ad identificare il firmatario. Deve essere inoltre creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo e essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica dei dati. La firma digitale, così come ne abbiamo discusso finora, è un tipo di firma elettronica avanzata che ha delle garanzie di robustezza tecnica che permettono di identificare il firmatario e garantire l'integrità del documento sulla base di un algoritmo matematico. Anche se la direttiva è tecnologicamente neutra – in altri termini non fa riferimento a procedure di cifratura particolari – essa indica essenzialmente le firme elettroniche basate su una infrastruttura a chiave pubblica (PKI).

La firma elettronica qualificata è una firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo per la creazione di una firma sicura. Il certificato qualificato è un certificato digitale che deve essere fornito da un prestatore di servizi di certificazione che soddisfa i requisiti dell'allegato II della medesima direttiva per quanto riguarda le modalità di emissione. In particolare questi allegati definiscono alcuni obblighi tra cui vale la pena di evidenziare i più significativi:

- la necessità di verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato

- la necessità di utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;

- la necessità di 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;

- la necessità di 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;

- la necessità di 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;

- la necessità di 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.

Questi obblighi perseguono anche un secondo obiettivo della direttiva che è quello di determinare il regime giuridico dei certificati di firma elettronica con lo scopo di assicurare la loro interoperabilità e la loro libera circolazione nel mercato interno (art. 4). Proprio per questo, la direttiva definisce uno standard minimo nel contenuto dei certificati qualificati (vedi allegato 1); i dati obbligatori sono specialmente l'identificazione del fornitore di servizi di certificazione, il nome del firmatario (o un suo pseudonimo), la durata di validità del certificato cosi come, all'occorrenza, tutti i limiti posti al suo utilizzo, quale ad esempio il valore massimo di una transazione. Da notare che il certificato deve essere firmato con la firma elettronica avanzata del suo fornitore. Quanto al firmatario, anche se la direttiva non lo precisa espressamente, non può essere che una persona fisica (conseguenza naturale dell'equivalenza con la firma autografa); naturalmente va da se che questa persona fisica può agire a nome e per conto di una persona giuridica.

Inoltre si rileva che, per il fatto stesso che il certificato possegga una "nazionalità" europea, i fornitori di certificati potrebbero fornire i loro servizi liberamente da un paese europeo all'altro (naturalmente soddisfacendo le direttive minime imposte dalla direttiva). Gli Stati membri non avrebbero il diritto di subordinare la loro attività ad autorizzazioni o a restrizioni. Inoltre, per rinforzare il sentimento di fiducia dei cittadini europei nel commercio elettronico, la direttiva istituisce un regime di responsabilità specifico e uniforme: i fornitori di certificati rispondono dei danni eventualmente subiti dalle persone che si sono affidate in buona fede ai dati contenuti nel certificato (art. 6).

Conformemente all'art. 12, la Commissione ha proceduto a una messa in opera della direttiva. Il suo rapporto pubblicato nel 2006[9], sottolinea che tutti gli stati membri si sono adeguati a grandi linee agli obblighi imposti dalla direttiva, specialmente per quanto riguarda l'argomento, fino ad allora contestato da alcuni paesi, dell'equivalenza della firma elettronica con la

[9] Relazione della Commissione al Parlamento europeo e al Consiglio - Relazione sull'attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (52006DC0120).

firma autografa. La Commissione deplora per contro che il mercato del commercio elettronico non si sia ancora sviluppato nella misura auspicata; a questo fornisce una spiegazione economica e non politica: "i prestatori di servizi hanno pochi incentivi a sviluppare la firma elettronica multiapplicazione, e preferiscono offrire soluzioni messe a punto per i propri servizi, come quelle elaborate dal settore bancario. Risulta in tal modo rallentato il processo di sviluppo di soluzioni interoperabili. L'assenza di applicazioni, come ad esempio le soluzioni globali per l'archiviazione elettronica, potrebbe anche impedire lo sviluppo di una firma multiruolo, che richiede una massa critica di utenti e di utenza".

## 10. La legislazione svizzera in tema di firma elettronica

### *10.1. Le fonti legislative*

La Svizzera, come risaputo, non è membro dell'Unione europea. Di conseguenza, giuridicamente parlando, essa non è tenuta alla messa in pratica della direttiva 1999/93 CE. Nonostante ciò la legislazione svizzera sulla firma elettronica si ispira ampiamente a questo testo. Il legislatore è stato cosciente del fatto che il commercio elettronico non riguarda un mercato nazionale, ma un mercato globale; di conseguenza si è prestata attenzione a non adottare standard divergenti che sarebbero stati di ostacolo al suo sviluppo. Resta il fatto che comunque il regime giuridico svizzero non ricalca esattamente il modello europeo: come avremo modo di constatare, su alcuni punti – certamente minori – definisce delle soluzioni differenti, in generale più restrittive, per garantire una sicurezza del diritto ottimale[10].

Il diritto svizzero sulla firma elettronica è fondato su due pilastri. Il primo è una modifica del Codice civile che mette sullo stesso piano la firma autografa con la firma elettronica (qualificata); il secondo è costituito da un insieme di testi di livello diverso che governano i servizi di certificazione. Il principale tra questi è la Legge federale del 19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica (vedi FiEle, RS 943.03[11]). Questo testo che è stato adottato nel 2003 –

[10] Sull'eurocompatibilità del diritto svizzero della firma elettronica, vedi il Foglio Federale 2001, p. 5140 ad 5.

[11] Vedi http://www.admin.ch/ch/i/rs/c943_03.html.

non senza controversie[12] – all'interno del Parlamento, è completato da un regolamento applicativo: l'Ordinanza del 3 dicembre 2004 sui servizi di certificazione nel campo della firma elettronica (vedi OFiEle, RS 943.032[13]). Infine le Prescrizioni amministrative dell'Ufficio federale delle comunicazioni, già modificate tre volte, forniscono le prescrizioni tecniche necessarie all'applicazione delle norme legislative. Queste prescrizioni si basano sugli standard internazionali in materia, in primo luogo le norme tecniche sulla scelta degli algoritmi e la lunghezza delle chiavi così come sulla marcatura temporale dell'*European Telecommunications Standards Institute*, norme seguite da numerosi paesi europei. Per questi motivi i certificati svizzeri sono perfettamente eurocompatibili.

### *10.2. Il processo telematico*

La Legge federale sui servizi di certificazione (FiEle), che è entrata in vigore il primo gennaio 2005, non ha scompigliato il diritto svizzero: i servizi di certificazione erano già governati dall'aprile 2000 – anche se facoltativamente – da una ordinanza "sperimentale" del Consiglio Federale il cui obiettivo era quello di assicurare, il più rapidamente possibile, la fornitura di servizi di certificazione sicuri a un largo pubblico. Il diritto attuale riprende in gran parte le soluzioni sperimentate – con un successo relativo, poiché in Svizzera come in Europa l'interesse per la firma elettronica è stato lento a manifestarsi[14] – utilizzando l'espediente di questa ordinanza provvisoria.

Il pezzo forte dell'intervento del legislatore è certamente il nuovo paragrafo 2*bis* dell'articolo 14 del Codice delle obbligazioni, che dà piena validità alla firma elettronica a patto che sia qualificata. Fino ad allora l'ar-

[12] Una minoranza dei parlamentari di sinistra riteneva che le regole sulla firma elettronica non avessero una propria autonomia ma dovessero essere inserite nella futura legge sul commercio elettronico, allora in preparazione. La maggioranza fu di avviso contrario. Fortunatamente, perché il progetto di legge sul commercio elettronico, giudicata troppo favorevole verso i consumatori, non ha ancora visto la luce.

[13] Vedi http://www.admin.ch/ch/i/rs/c943_032.html.

[14] A tal punto che l'unico fornitore di servizi di certificazione, SwissKey ha fatto fallimento nel 2001 a causa del limitato numero di clienti. Questo disinteresse ha una sua spiegazione con il fatto che le banche svizzere, che dovevano essere i principali clienti, hanno alla fine sviluppato autonomamente i loro sistemi di identificazione e di autenticazione.

ticolo 14 del CO ammetteva solamente la firma autografa. Una chiarificazione legislativa tanto più necessaria poiché la giurisprudenza si era mostrata poco flessibile, rifiutando a più riprese il riconoscimento come documenti validi di prodotti delle nuove tecnologie quali il telex[15] o il fax[16]. Il tenore del nuovo articolo è il seguente: "La firma elettronica qualificata fondata su un certificato qualificato di un prestatore riconosciuto di servizi di certificazione ai sensi della legge del 19 dicembre 2003 sulla firma elettronica è equiparata alla firma autografa. Sono fatte salve le disposizioni legali o contrattuali contrarie".

Possiamo subito costatare che il legislatore ha definito un'equivalenza quasi assoluta, sotto riserva di disposizioni contrattuali contrarie. Numerosi parlamentari hanno nel frattempo auspicato maggiori possibilità di deroga, sull'esempio della direttiva europea 1999/93. In particolare hanno preconizzato il mantenimento della necessità della sola firma autografa nei settori sensibili dal lavoro, dei contratti di locazione, del diritto dei consumatori e del leasing alfine di proteggere le parti più deboli contro degli impegni presi in modo irriflessivo. Questo punto di vista è stato largamente battuto[17].

Consacrando la firma elettronica qualificata il legislatore ha optato per una tecnologia più pesante con il rischio di scoraggiare alcuni utilizzatori. In tutti i casi era importante accordare il valore *giuridico* solo ai procedimenti che offrivano le più alte garanzie di sicurezza. Per il resto il diritto svizzero non impone la firma qualificata nelle transazioni commerciali. È lasciata facoltà agli attori economici di organizzare come meglio credono le loro transazioni commerciali elettroniche; tuttavia nel caso in cui la firma autografa è la condizione per la validità della transazione, la firma elettronica sarà accettata solo se soddisferà le condizioni poste dall'articolo 14 par. 2*bis*.

L'ormai chiara equiparazione della firma elettronica alla firma autografa è un passo in avanti la cui importanza non deve essere tuttavia sopravalutata. In effetti, nel diritto svizzero prevale ancora largamente il principio della libertà della forma dei contratti (art. 11 par. 1 CO). Ciò significa che per la

[15] DTF 112 II 326ss.

[16] DTF 121 II 252ss.

[17] Per 105 consiglieri nazionali contro 57 (Bollettino ufficiale del Parlamento 2003 N 821).

maggior parte dei contratti non è prescritta nessuna forma speciale: può essere sufficiente un accordo verbale o uno scambio di messaggio di posta elettronica. È solo in alcuni casi che il legislatore impone una forma particolare: scritta, o addirittura autenticata. La forma scritta è soprattutto richiesta la dove è importante assicurarsi o che le parti non si siano comportate in modo irriflessivo o per proteggere il consumatore senza esperienza, come nel caso del credito al consumo o nelle vendite con pagamento anticipato.

Naturalmente nelle transazioni in cui la forma scritta autenticata è imperativamente richiesta (in particolar modo la vendita di beni immobiliari) la firma elettronica non entra in considerazione. Si impone la presenza di un notaio.

Il titolare di una chiave di firma è tenuto a sorvegliare che la sua chiave non sia utilizzata abusivamente. A questo proposito sono definiti degli obblighi specifichi di sicurezza (art. 11 OFiEle):

"1. I titolari di certificati qualificati non devono affidare a nessuna altra persona il dispositivo per la creazione della firma. Nella misura in cui sia ragionevolmente esigibile, lo portano con sé o lo conservano sotto chiave.

2. In caso di perdita o di furto del dispositivo per la creazione della firma, il titolare del certificato qualificato ne deve chiedere senza indugio l'annullamento. Lo stesso vale se il titolare sa o ha il sospetto fondato che un terzo abbia potuto avere accesso alla chiave per la creazione della firma.

(…)

4. Le trascrizioni dei dati di attivazione devono essere conservate in un luogo sicuro e separatamente dal dispositivo per la creazione della firma.

5. Il titolare di un certificato qualificato modifica i dati di attivazione se sa o se ha il sospetto fondato che un terzo ne sia venuto a conoscenza. Se non può modificare egli stesso i dati di attivazione deve chiedere senza indugio l'annullamento del certificato".

Il mancato rispetto di uno di questi obblighi può avere delle gravi conseguenze civili: in virtù del nuovo articolo 59a CO il titolare di una chiave di firma deve riparare i danni subiti da terzi che si sono fidati, in buona fede, di un certificato qualificato caduto in cattive mani. Non può esimersi dalle sue responsabilità se non mostrando in modo credibile di aver preso tutte le misure di sicurezza prescritte.

Per quanto riguarda le autorità di certificazione, la legislazione svizzera prevede un sistema complesso a tre livelli: i fornitori di servizi di certifica-

zione, gli organismi di riconoscimento dei fornitori di servizi di certificazione e infine l'organismo di accreditamento degli organismi di riconoscimento.

Il ruolo fondamentale è assicurato dai fornitori di servizi di certificazione. In effetti è a loro che incombe il compito di fornire i certificati qualificati che attestano che la chiave di verifica di una firma è legata a una precisa persona. A questo scopo gli articoli 8 FiEle e art. 5 OFiEl impongono loro dei doveri precisi di verifica; devono naturalmente assicurarsi dell'identità della persona e esigere la sua presenza fisica e la produzione di un documento di identità[18]. D'altra parte devono costantemente preoccuparsi di adattare i loro prodotti al progresso tecnico; l'art. 3 dell'ordinanza prevede in effetti che: "certificati qualificati sono rilasciati soltanto se la lunghezza della chiave per la creazione e per la verifica della firma e il tipo di algoritmo riconosciuto utilizzato sono tali da resistere agli attacchi crittografici durante la validità del certificato qualificato".

Infine, va notato che i fornitori di servizi devono informare i loro clienti sulle responsabilità (vedi sopra) a cui possono andare incontro nel caso di utilizzo abusivo o di perdita della loro chiave di firma così come della necessità di assicurare la sua confidenzialità (art. 9 FiEle).

A tutt'oggi (ottobre 2007), sono stati riconosciuti quattro fornitori di servizi di certificazione[19]: tre aziende private (Swisscom Solutions AS, QuoVadis Trustlink et SwissSign SA) e una autorità pubblica (l'Ufficio federale dell'informatica e della telecomunicazione). Tutti questi fornitori sono svizzeri. In teoria nulla vieta che un fornitore di servizi estero possa operare in Svizzera; deve tuttavia far convalidare il suo riconoscimento straniero dall'organismo di riconoscimento svizzero; quest'ultimo non procederà ad una valutazione completa dell'organizzazione e delle infrastrutture del richiedente ma si accontenterà di esaminare in quale misura le condizioni di fornitura del riconoscimento (regole di fondo idoneità dell'organismo straniero) siano equivalenti alla regolamentazione svizzera.

Il ruolo degli organismi di riconoscimento è di garantire che i fornitori di servizi siano in grado di esercitare le loro attività conformemente alla

[18] Come nel diritto europeo, anche nel diritto svizzero i certificati possono essere forniti solo alle persone fisiche.

[19] Vedi http://www.seco.admin.ch/sas/00229/00251/.

legislazione sulla firma elettronica (art. 4 FiEle). È importante sottolineare che, anche se il riconoscimento non ha valore di decisione amministrativa, la relazione che si stabilisce tra il fornitore e l'organismo di riconoscimento è retto dal diritto pubblico; ciò significa che un candidato fornitore di servizi che soddisfa le condizioni legali ha automaticamente diritto al riconoscimento, indipendentemente dall'opinione dell'organismo di riconoscimento.

Per ora è accreditato un solo organismo di riconoscimento e si tratta della società fiduciaria KPMG.

Da ultimo il compito di accreditare gli organismi di riconoscimento è stato conferito dall'art. 1 OFiEle ad un'autorità pubblica, il Servizio di accreditamento svizzero dell'Ufficio federale di metrologia e di accreditamento.

La Legge federale sui servizi di certificazione (FiEle) tratta l'utilizzo della firma elettronica nelle relazioni tra privati. Non considera questo strumento nel contesto dell'amministrazione elettronica (*e-government*) o della procedura giudiziaria. Nonostante ciò il legislatore, per motivi di coerenza, si è in seguito preoccupato che i certificati emessi dai certificatori riconosciuti ai sensi della Legge federale sui servizi di certificazione (FiEle) fossero determinanti per entrare in relazioni con le autorità pubbliche.

È così che dal primo gennaio 2007 è possibile depositare dei ricorsi in modo elettronico presso il Tribunale federale[20]. Allo stesso modo, il prossimo primo gennaio 2008, anche le procedure amministrative nei confronti delle autorità federali potranno essere gestite in forma elettronica[21].

[20] Per maggiori dettagli vedere gli artt. 42 capoverso 4 e 60 capoverso 3 della legge del 17 giugno 2005 sul Tribunale federale (RS 173.110) e art. 2 regolamento del Tribunale federale del 5 dicembre 2006 sulla comunicazione elettronica con le parti e le autorità precedenti (RS 173.110.29).

[21] Artt. 11b capoverso 2, 21a capoverso 1 e 34 capoverso 1-*bis* della legge federale del 20 dicembre 1968 sulla procedura amministrativa e l'art. 2 dell'ordinanza del 17 ottobre 2007 concernente la comunicazione per via elettronica nell'ambito di una procedura amministrativa.

Sulle comunicazioni elettroniche e sulle firme digitali da utilizzare nella procedura giudiziaria, v. ampiamente in questo volume, T. Koller e M. Rey.