LEGGE 20 luglio 2005 n.115

REPUBBLICA DI SAN MARINO

LEGGE SUL DOCUMENTO INFORMATICO E LA FIRMA ELETTRONICA

Noi Capitani Reggenti
la Serenissima Repubblica di San Marino

Promulghiamo e mandiamo a pubblicare la seguente legge approvata dal Consiglio Grande e Generale nella seduta del 20 luglio 2005.

Art. 1
(Definizioni)

1. Ai fini della presente legge, valgono le seguenti definizioni:
   a) "documento amministrativo", ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;
   b) "documento informatico", la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
   c) "firma elettronica" ("digital signature"), dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di validazione;
   d) "firma elettronica avanzata", una firma elettronica ottenuta attraverso una procedura informatica, che soddisfi i seguenti requisiti:
      I. essere connessa in maniera unica al firmatario;
      II. essere idonea ad identificare il firmatario;
      III. essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
      IV. essere collegata ai dati cui si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
   e) "firma elettronica qualificata", una firma elettronica avanzata che sia basata su di un certificato qualificato creato mediante un dispositivo sicuro per la creazione della firma;
   f) "firmatario", una persona che ha accesso al dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;
   g) "dati per la creazione di una firma", dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;
   h) "dispositivo per la creazione di una firma", un software configurato o un hardware usato per utilizzare i dati per la creazione di una firma;
   i) "dispositivo sicuro per la creazione di una firma", un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'articolo 7;
   l) "dati per la verifica della firma", dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;

m) "servizio di firma e certificazione", la messa a disposizione di prodotti e procedure necessarie per la firma, l'emissione, il rinnovo e la gestione di certificati, servizi elenchi, servizi di revoca, servizi di registrazione e servizi di time stamping, nonché servizi informatici e di consulenza correlati alle firme elettroniche;

n) "dispositivo di verifica della firma", un software configurato o un hardware usato per utilizzare i dati di verifica della firma, secondo le raccomandazioni di cui al successivo articolo 8;

o) "certificato", un attestato elettronico che collega i dati di verifica della firma ad un titolare e conferma l'identità di tale titolare;

p) "certificato qualificato", un certificato elettronico conforme ai requisiti di cui all'articolo 4 rilasciato da un prestatore di servizi di certificazione che risponde ai requisiti di cui all'articolo 5;

q) "prestatore di servizi di certificazione" o "certificatore", un organismo o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;

r) "prodotto di firma elettronica", hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche;

s) "validazione temporale" o "time stamping", il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile a terzi;

t) "servizio di time stamping", una attestazione recante la firma elettronica di un certificatore che comprova l'esistenza di determinati dati elettronici in un determinato momento (data ed orario).

Art. 2

(Documento informatico e sua validità)

1. Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione su supporto informatico e trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, purché firmati e validati ai sensi della presente legge.

2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate sia il soggetto che ha effettuato l'operazione.

3. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

4. Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici saranno stabilite con specifici regolamenti tecnici da emanare mediante decreto reggenziale.

Art. 3

(Effetti giuridici delle firme elettroniche)

1. L'uso di una firma elettronica apposta o associata mediante certificato revocato o scaduto equivale alla mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione da parte dei prestatori di servizi di certificazione.

2. La trasmissione del documento informatico per via telematica, firmato elettronicamente ai sensi dei regolamenti previsti dalla presente legge, con modalità che assicurino l'avvenuta consegna, equivale alla spedizione per mezzo posta.

3. Le firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma:

a) posseggono i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per i dati cartacei;
b) sono ammesse come prova in giudizio.

4. La firma elettronica non può essere considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:

- in forma elettronica, o
- non basata su un certificato qualificato, o
- non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero
- non creata da un dispositivo sicuro per la creazione di una firma.

5. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi ai regolamenti tecnici previsti dalla presente legge.

6. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente, si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se conformi ai regolamenti tecnici previsti dalla presente legge.

Art. 4

(Requisiti relativi ai certificati qualificati)

1. I certificati qualificati devono includere almeno le seguenti informazioni:

a) l'indicazione che il certificato rilasciato è un certificato qualificato;
b) l'identificazione del prestatore di servizi di certificazione e lo Stato in cui ha la propria sede;
c) il nome del firmatario 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 qualificata del prestatore di servizi di certificazione che ha rilasciato il certificato;
i) i limiti d'uso del certificato, ove applicabili;
l) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

Art. 5

(Requisiti relativi al prestatore di servizi di certificazione che rilascia certificati qualificati)

1. Il prestatore di servizi di certificazione che rilascia certificati qualificati deve:

a) dimostrare l'affidabilità organizzativa tecnica e finanziaria necessaria per fornire servizi di certificazione;

b) assicurare il funzionamento di un servizio di gestione delle informazioni puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;

c) utilizzare nei certificati qualificati e per i servizi elenchi e per i servizi di revoca un time stamping di qualità garantita, e comunque assicurare la localizzazione temporale dell'emissione e della revoca di un certificato qualificato;

d) verificare con mezzi appropriati, l'identità e, eventualmente, le specifiche caratteristiche della persona cui viene 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 di 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, l'integrità e la sicurezza nel corso della generazione di tali dati;

h) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla legge, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione di responsabilità civile;

i) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un periodo di almeno 10 anni, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;

l) 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;

m) prima di avviare un rapporto 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 e le procedure di reclamo e di 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;

n) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:

   I. soltanto le persone autorizzate possano effettuare inserimenti e modifiche;

   II. l'autenticità delle informazioni sia verificabile;

   III. i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato;

   IV. l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

Art. 6

(Responsabilità)

1. Il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico l'affidabilità di tale certificato, è responsabile per

danni provocati a entità o persone fisiche o giuridiche che facciano ragionevole affidamento su detto certificato:

a) per quanto riguarda l'esattezza di tutte le informazioni contenute nel certificato qualificato dal momento del rilascio e il fatto che esso contenga tutti i dati prescritti per un certificato qualificato,

b) per la garanzia che, al momento del rilascio del certificato, il firmatario identificato nel certificato qualificato detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato,

c) per la garanzia che i dati per la creazione della firma e i dati per la verifica della firma possano essere usati in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi entrambi,

a meno che il prestatore di servizi di certificazione provi di aver agito senza negligenza.

2. Il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato è responsabile, nei confronti di entità o di persone fisiche o giuridiche che facciano affidamento sul certificato, dei danni provocati, per la mancata registrazione della revoca del certificato, a meno che provi di aver agito senza negligenza.

3. Un prestatore di servizi di certificazione ha la facoltà di indicare, in un certificato qualificato, i limiti d'uso di detto certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione è esentato dalla responsabilità per i danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti nello stesso.

4. Un prestatore di servizi di certificazione ha la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione non è responsabile dei danni risultanti dal superamento di detto limite massimo.

5. Il prestatore di servizi di certificazione deve poter fornire, su richiesta, la marcatura temporale (time stamping), di adeguata precisione, di cui assicurerà la tenuta della registrazione per un congruo numero di anni come indicato da decreto reggenziale di cui all'articolo 2, punto 4.

6. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 5; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto reggenziale, saranno definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

Art. 7

(Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata)

1. I dispositivi per la creazione di una firma elettronica qualificata, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che:

a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è garantita la loro riservatezza;

b) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro i limiti di sicurezza previsti, essere derivati e la firma è protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile;
c) i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi sicuri per la creazione di una firma non devono alterare i dati da firmare né impedire che tali dati siano presentati al firmatario prima dell'operazione di firma; deve inoltre essere richiesta, senza ambiguità, la volontà di generare la firma.

Art. 8

(Raccomandazioni per la verifica della firma elettronica qualificata)

1. Durante il processo relativo alla verifica della firma elettronica qualificata occorre garantire, entro limiti di certezza, che:
a) i dati utilizzati per la verifica della firma corrispondono ai dati comunicati al verificatore;
b) la firma è verificata in modo affidabile e i risultati della verifica correttamente comunicati;
c) il verificatore può, all'occorrenza, stabilire in modo attendibile i contenuti dei dati firmati;
d) l'autenticità e la validità del certificato necessario al momento della verifica della firma sono verificate in modo attendibile;
e) i risultati della verifica e dell'identità del firmatario sono comunicati correttamente;
f) l'uso di uno pseudonimo è chiaramente indicato;
g) qualsiasi modifica che incida sulla sicurezza può essere individuata.

Art. 9

(Settore Pubblico)

1. All'interno della Pubblica Amministrazione e Settore Pubblico Allargato e per le comunicazioni tra organismi statali e persone fisiche o giuridiche, l'uso della firma elettronica può essere soggetto a requisiti specifici che saranno individuati dal regolamento tecnico da emanare mediante il decreto reggenziale di cui all'articolo 2, punto 4.

Art. 10

(Organismo tecnico)

1. Le competenze tecniche di attuazione della presente legge vengono espletate dall'Autorità per l'Informatica di cui alla Legge 23 maggio 1995 n.70, che si avvale del supporto tecnico dell'Ufficio Programmazione Economica Centro Elaborazione Dati e Statistica ed eventualmente della consulenza di persone o società esperte nelle problematiche concernenti la firma elettronica.

Art. 11

(Compiti affidati all'Autorità per l'Informatica)

1. E' compito dell'Autorità per l'Informatica promuovere i regolamenti tecnici da emanare con il decreto reggenziale di cui all'articolo 2, punto 4. Tali regolamenti dovranno tener conto degli standard emergenti a livello internazionale.

2. Almeno ogni due anni, a partire dalla pubblicazione del regolamento tecnico, l'Autorità per l'Informatica provvede ad esaminare i progressi tecnologici, l'evoluzione del mercato e gli sviluppi

giuridici a livello internazionale e provvede, se del caso, ad apportare le opportune modifiche al regolamento tecnico.

3. Ogni sei mesi, a partire dalla pubblicazione del regolamento tecnico, l'Autorità per l'Informatica provvede a pubblicare una lista degli Stati terzi la cui normativa sulla firma elettronica risulta conforme ai requisiti indicati nella presente legge e del regolamento tecnico.

4. E' compito dell'Autorità per l'Informatica, con il supporto tecnico dell'Ufficio Programmazione Economica Centro Elaborazione Dati e Statistica ed eventualmente della consulenza di persone o società esperte nelle problematiche concernenti la firma elettronica, svolgere funzioni di vigilanza e controllo sulle attività di certificazione e rilascio dei certificati svolte da parte del prestatore di servizi di certificazione.

Art. 12
(Aspetti internazionali)

1. Al fine di agevolare servizi di certificazione transfrontalieri con Paesi terzi e il riconoscimento giuridico delle firme elettroniche qualificate che hanno origine in Paesi terzi, l'Autorità per l'Informatica presenta, se del caso, proposte miranti all'effettiva attuazione di norme e di accordi internazionali applicabili ai servizi di certificazione.

Art. 13
(Protezione dei dati)

1. Il prestatore di servizi di certificazione e gli organismi responsabili dell'accreditamento o della supervisione si devono conformare alla Legge 23 maggio 1995 n. 70 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

2. È consentito a un prestatore di servizi di certificazione che rilascia certificati al pubblico di raccogliere dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Art. 14
(Riesame)

1. Ogni due anni, a partire dall'entrata in vigore della presente legge, l'Autorità per l'Informatica riesamina l'applicazione della presente legge e presenta una relazione in merito al Consiglio Grande e Generale.

2. Nel riesame si valuta, tra l'altro, se l'ambito di applicazione della presente legge debba essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. La relazione è corredata, se del caso, di proposte legislative.

Art. 15
(Entrata in vigore)

1. La presente legge entra in vigore il quinto giorno successivo a quello della sua legale pubblicazione.

Data dalla Nostra Residenza, addì 25 luglio 2005/1704 d.F.R

I CAPITANI REGGENTI
Fausta Simona Morganti - Cesare Antonio Gasperoni

IL SEGRETARIO DI STATO
PER GLI AFFARI INTERNI
Rosa Zafferani