SOMMARIO

ALLEGATO A

ALLEGATO B

1.
INTRODUZIONE

L'Italia è stata tra i primi Paesi al mondo a dotarsi di una legislazione estesa in materia di firma digitale. La normativa è stata modificata numerose volte sia per motivi derivanti dall'evoluzione delle transazioni elettroniche sia per adeguarsi alla normativa comunitaria.

Il punto di partenza è nell'articolo 15, comma 2 della Legge 15 marzo 1997, n. 59 recante la "Delega al Governo per il conferimento di funzioni e compiti alle Regioni e agli Enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa", che introduce nella normativa nazionale il principio generale della validità e della rilevanza giuridica delle rappresentazioni informatiche.

Il comma stabilisce che «gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge». La norma nasce per disciplinare il valore giuridico degli atti della pubblica amministrazione trasmessi telematicamente sulla nascente R.U.P.A., la Rete Unitaria della Pubblica Amministrazione.

Con il trascorrere degli anni e con lo sviluppo delle telecomunicazioni, e in particolare con la diffusione di massa della rete Internet e con l'utilizzo del commercio elettronico, il concetto

di firma si è evoluto, ampliato e differenziato sempre di più da quello noto nei secoli di firma autografa. La normativa nazionale ha recepito prima la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche; poi si è coordinata con il regolamento europeo 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni nel mercato interno e che abroga la direttiva 1999/93/CE.

Questo regolamento è generalmente noto come "Regolamento eIDAS".

La natura dello strumento giuridico prescelta dall'Unione Europea, cioè quella del regolamento e non di direttiva, ha avuto un impatto sul sistema. Il regolamento è direttamente applicabile in tutti gli Stati membri dell'Unione europea, senza la necessità di atti di recepimento nei singoli Stati membri. Quindi il regolamento non è uno strumento di armonizzazione ma costituisce uniformazione del diritto per gli Stati membri con l'obiettivo di eliminare alla radice, almeno nelle previsioni, quelle piccole differenze che limitano il compiersi di un mercato unico per i servizi della società dell'informazione e della comunicazione.

In questo scenario storico e normativo il presente volume ha l'obiettivo di descrivere in tono divulgativo ma non semplicistico le firme informatiche. Questa espressione tratta da [7] è volutamente utilizzata in senso non tecnico, al fine di includere tutte le differenti fattispecie di firme elettroniche a partire dalla firma digitale che è stata la prima definita nell'ordinamento nazionale.

Il capitolo successivo descrive la struttura del libro.

2.
STRUTTURA DEL LIBRO

Questo libro ha l'obiettivo di essere fruibile dal lettore poco esperto, da quello che vuole trovare riferimenti normativi sulla materia, dal tecnico che ha necessità di approfondire i temi – quasi mai trattati – delle strutture tecnologiche di riferimento delle firme. Vengono affrontate le tematiche in modo prima introduttivo per poi approfondire la parte legale e quella tecnica.

Un simbolo **!** (punto esclamativo in colore rosso) evidenzia un capitolo o paragrafo contenente un argomento più complesso per il lettore medio; un capitolo o un paragrafo con **!!** (due punti esclamativi in colore rosso) tratta di argomenti di natura tecnica per specialisti che vogliono approfondire una serie di dettagli nel settore delle firme elettroniche e della tecnologia ad esse associata.

Il contenuto del libro è descritto nel seguito con una sintesi dei contenuti di ogni capitolo.

Il capitolo 3 contiene un'introduzione generale alle firme informatiche. Con questo termine si aggregano tutte le tipologie di firme definite nella normativa nazionale ed europea.

Il capitolo 4 tratta della normativa delle firme informatiche con il regolamento europeo 910/2014 (eIDAS), i prestatori di servizi fiduciari e l'impatto di questa normativa sull'ordinamento nazionale.

Il capitolo 5 introduce la tecnologia delle firme informatiche,

descrivendo in modo discorsivo la crittografia, le funzioni crittografiche applicate nello specifico settore e qualche applicazione generale delle stesse.

Il capitolo 6 descrive alcune caratteristiche generali delle firme informatiche e come queste caratteristiche possono essere utilizzate nelle applicazioni reali.

Il capitolo 7 introduce le definizioni delle firme informatiche derivate dalla normativa comunitaria e da quella nazionale.

Il capitolo 8 riprende i temi normativi generali sulle firme e approfondisce gli effetti giuridici delle firme informatiche.

Il capitolo 9 approfondisce le funzioni delle firme e ne descrive anche funzioni operative, comprendendo anche la fattispecie del sigillo elettronico. In questo capitolo viene discussa la firma grafometrica.

Il capitolo 10 descrive le numerose modalità di sottoscrizione con attenzione alla firma remota e particolari applicazioni, come la cosiddetta firma con certificato "usa e getta".

Il capitolo 11 tratta in modo generale gli standard tecnici di riferimento un Europa, sia in applicazione del regolamento europeo eIDAS che delle specifiche della rete Internet stabilite con gli IETF RFC.

Il capitolo 12 si rivolge agli utenti che utilizzano le firme, mostrando in modo visivo una serie di applicazioni di firma e il loro utilizzo. In questo capitolo si tratta del cruciale problema della verifica delle sottoscrizioni.

Il capitolo 13 illustra il tema dell'interoperabilità delle firme in Europa.

Il capitolo 14 offre una visione sintetica sugli scenari di utilizzo delle firme informatiche con particolare attenzione alla descrizione di alcuni termini tipici del mondo "cartaceo", che possono essere applicati anche al mondo digitale.

Il capitolo 15, analogamente al capitolo precedente, tratta degli scenari di utilizzo dei sigilli elettronici.

Il capitolo 16 introduce il tema dell'esigenza dell'aggiornamento delle regole tecniche sulle firme, delineando una proposta per delle Linee guida sul tema.

Il capitolo 17 esamina alcuni luoghi comuni sulle firme confermandoli o, nella maggior parte dei casi, smentendoli.

Il libro si chiude con i classici riferimenti bibliografici, sitografici e normativi e con due allegati tecnici. La bibliografia e la sitografia sono utilizzate nel testo con la notazione [n]. Nel volume quando si fa riferimento a un testo o ad un sito si indica lo specifico numero di riferimento. Una serie di riferimenti sono indicati per chi volesse approfondire temi tecnici storici o particolari. Questi non hanno una citazione diretta nel testo ma sono la base storica di quanto qui trattato come ad esempio [1], [2] e [5].

Nell'allegato A sono descritti gli aspetti generali della sintassi ASN.1 e degli identificatori di oggetti, che rappresentano due argomenti la cui conoscenza è indispensabile per chi vuole approfondire le strutture dati utilizzate per le firme informatiche.

Nell'allegato B sono mostrate alcune strutture dati relative a certificati digitali, marche temporali e profili di firma.

Definizioni e acronimi

AES	Advanced Encryption Standard
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale (D.Lgs. n.82/2005)
CAdES	Cryptographic message syntax Advanced Electronic Signature

CEN	Comité Européen de Normalisation - Comitato Europeo di Normazione
CIE	Carta di Identità Elettronica
CNS	Carta Nazionale dei Servizi
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Practice Statement
eIDAS	electronic Identification Authentication and Signatureregulation
ETSI	European Telecommunications Standards Institute
FEA	Firma Elettronica Avanzata
FEQ	Firma Elettronica Qualificata
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
IETF	Internet Engineering Task Force
OCSP	On-line Certificate Status Protocol
OID	Object IDentifier
PAdES	PDF Advanced Electronic Signature
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
QSealC	Qualified Electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
SSCD	Secure Signature Creation Device
TS-CNS	Tessera Sanitaria con CNS
TSA	Time Stamping Authority
TSU	Time Stamping Unit
TSL	Trust-service Status List
XAdES	XML Advanced Electronic Signature