3. Le firme elettroniche

Nel mondo analogico, si era abituati a conoscere ed usare un unico tipo di firma, ossia quella autografa apposta sulla carta, e si è abituati a riconoscerle il significato giuridico per il quale l'apposizione di essa in calce ad una dichiarazione ha lo scopo di attestare - fino a prova contraria - la provenienza delle dichiarazioni in esso contenute.
Con l'avvento delle firme elettroniche si deve modificare il modo di intendere il concetto di sottoscrizione.
Le firme elettroniche non riproducono il nome e il cognome del firmatario, non sono costituite da parole, né da disegni, non sono apposte manualmente; si tratta piuttosto di sottoscrizioni che, in forma di bit, conferiscono determinati effetti ad un dato documento informatico.
Il Codice dell'Amministrazione Digitale disciplina le tipologie di firme elettroniche e la loro efficacia giuridica nell'ambito dell'attività amministrativa e negoziale.

L'evoluzione del quadro normativo in materia di firme elettroniche

Con l'avvento delle firme elettroniche si deve modificare il modo di intendere il concetto di sottoscrizione.
Le firme elettroniche non riproducono il nome e il cognome del firmatario, non sono costituite da parole, né da disegni, non sono apposte manualmente; si tratta piuttosto di sottoscrizioni che, in forma di bit, conferiscono determinati effetti ad un dato documento informatico.

In linea generale, la sottoscrizione elettronica consiste in una serie di informazioni digitali apposte o collegate ad un documento (in senso lato) utilizzate come metodo di identificazione informatica.
La sottoscrizione elettronica, analogamente a quanto accade per la firma autografa sui documenti cartacei, è l'elemento (informatico) che permette di attribuire all'autore la paternità giuridica del documento.

Il Codice dell'Amministrazione Digitale, innovando la materia delle firme, ha uniformato il sistema della sottoscrizione elettronica al quadro comunitario per le firme elettroniche tracciato dalla Direttiva 1999/93/CE. L'assetto delineato dal CAD ha trovato specificazione nel Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 che individua caratteristiche e condizioni di operatività delle diverse tipologie di firma previste dalla normativa.

Nello scenario attuale, quindi, sono previste quattro tipologie di firma, che assicurano differenti livelli sicurezza, alle quali sono riconosciuti differenti effetti giuridici: conseguentemente ad ogni tipologia di firma viene ricondotto un diverso valore probatorio.

Proprio sulla differente valenza giuridica e probatoria dei diversi tipi di firma si fonda la classificazione delle diverse tipologie di firme elettronica in due macro-tipologie:

a) firme deboli (firma elettronica): consentono di ricondurre il documento ad un soggetto con un certo grado di "affidabilità" (variabile da caso a caso) senza garantire l'integrità del documento stesso. La loro "affidabilità" è strettamente legata alle caratteristiche intrinseche dei sistemi utilizzati. Per questo motivo, il documento cui è apposta una firma elettronica è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
b) firme forti (firma elettronica avanzata, firma elettronica qualificata e firma digitale) sono quelle per cui il firmatario non può disconoscere semplicemente la sottoscrizione ma si rende necessaria la querela di falso. Queste firme garantiscono l'identità dell'autore e l'integrità del documento firmato.

Le firme elettroniche previste dal CAD

Il Codice dell'Amministrazione Digitale, nel quale le firme elettroniche trovano la loro più completa disciplina, distingue ben quattro tipologie di firme informatiche:

1. Firma elettronica

Con l'espressione firma elettronica s'intende un insieme di dati in forma elettronica, riconducibili all'autore (anche di tipo: log identificativo, indirizzo mail, ecc.), allegati oppure connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica. La firma

elettronica quindi, più che a una vera e propria firma, dà vita ad un processo di autenticazione cui sono riferibili minori requisiti di sicurezza rispetto alle altre firme (le c.d. forti)

La normativa riconosce alla firma elettronica un valore probatorio: la firma è liberamente valutabile dal giudice in fase di giudizio, in base a caratteristiche oggettive di qualità e sicurezza.

2. Firma elettronica avanzata

È un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garantisce integrità (consentendo di rilevare se i dati sono stati successivamente modificati), autenticità del documento sottoscritto. La sua creazione presuppone l'utilizzo di mezzi sui quali il firmatario mantiene il controllo esclusivo. Quest'ultimo elemento assicura la connessione univoca con il firmatario e quindi la paternità giuridica del documento.

La firma elettronica avanzata presenta dei caratteri peculiari che la differenziano marcatamente rispetto alle altre tipologie di firma. In primo luogo, la normativa non vincola la firma elettronica avanzata a particolari standard tecnici o determinati *software*. Conseguentemente non esiste uno standard di firma elettronica avanzata, ma sono ipoteticamente possibili soluzioni di firma anche molto diverse tra loro, purché rispettino i requisiti richiesti dalla legge:

1) capacità di assicurare integrità ed autenticità del documento sottoscritto;
2) controllo esclusivo del dispositivo di firma da parte del firmatario.

Gli strumenti più diffusi sono quelli che utilizzano nei processi di sottoscrizione le parole d'ordine temporanee (*one time password* - OTP) e i dati biometrici, tra cui assumono un posto di rilievo le soluzioni di firma grafometrica.

In secondo luogo, l'offerta di soluzioni di firma elettronica avanzata, che non richiede alcuna autorizzazione preventiva, è possibile da parte di tutti i soggetti che intendono utilizzarla nei rapporti con terze parti per motivi istituzionali, societari o commerciali e dalla pubblica amministrazione.

Questi soggetti possono:

- erogare direttamente soluzioni di firma elettronica avanzata realizzate in proprio;
- mettere a disposizione dei propri interlocutori di soluzioni di firma acquistate sul mercato.

Il documento informatico sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, è riconosciuto valido fino a querela di falso. Pertanto, questa tipologia di firma comporta l'inversione dell'onere della prova: chi intende disconoscere la sottoscrizione di un documento dovrà provare che l'apposizione della firma è riconducibile ad altri e che tale apposizione non è imputabile a sua colpa.

Appare importante sottolineare come il legislatore abbia deciso di limitare l'ambito di validità della firma elettronica avanzata ai soli rapporti intercorrenti tra il sottoscrittore e il soggetto l'erogatore della soluzione di firma.

3. Firma elettronica qualificata

È un particolare tipo di firma elettronica avanzata basato su un certificato "qualificato" (che garantisce l'identificazione univoca del titolare, rilasciato da certificatori accreditati) e realizzato mediante un dispositivo sicuro per la generazione della firma che soddisfa particolari requisiti di sicurezza; il certificato può contenere limitazioni relative alla tipologia di atti da sottoscrivere o a tetti di spesa.

4. Firma digitale

È un particolare tipo di firma elettronica avanzata basato su un certificato qualificato e su un sistema di doppia chiave crittografica, una pubblica (contenuta nel certificato qualificato) ed una privata (custodita dal mittente) che, nel loro uso congiunto, servono a garantire e a verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Il documento informatico sottoscritto con firma elettronica qualificata o firma digitale, formato nel rispetto delle regole tecniche, è riconosciuto valido a tutti gli effetti di legge e soddisfa il requisito della forma scritta, secondo quanto previsto dall'art 1350 c.c., punti 1-12. Le elevate garanzie di sicurezza connesse comportano, anche per queste tipologie di firme, l'inversione dell'onere della prova, per cui chi intende disconoscere la sottoscrizione di un documento dovrà provare che l'apposizione della firma è riconducibile ad altri e che detta apposizione non è imputabile a sua colpa.

Dal punto di vista tecnico-operativo, le operazioni da compiere per apporre la firma ad un documento informatico possono variare in base al *software* di firma utilizzato. I tratti fondamentali, però, sono comuni a tutti gli applicativi utilizzati:

- il *software* di firma richiede di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore o la "chiavetta" nella porta USB;
- successivamente il software chiede l'inserimento del codice PIN e salva il documento sottoscritto e pronto per essere utilizzato. Nel caso in cui il processo di firma interessi un numero elevato di documenti è possibile automatizzare le procedure di sottoscrizione purché l'operazione di firma automatizzata si svolga nel rispetto della normativa tecnica vigente. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Rispetto ai documenti informatici su cui è apposta firma digitale si pone, quindi, il problema della verifica della firma digitale. In particolare, occorre accertare che:

– il documento non sia stato modificato dopo la firma;

– il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;

– il certificato del sottoscrittore non sia scaduto;

– il certificato del sottoscrittore non sia stato sospeso o revocato.

Il CAD, all'art. 25, disciplina, inoltre, la firma elettronica autenticata. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata, consiste nell'attestazione, da parte del pubblico ufficiale (es. Notaio), che:

– la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale;

– l'eventuale certificato elettronico utilizzato risulta valido;

–il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

Questa firma è equiparata, ai fini di legge, alla sottoscrizione autenticata dal notaio o da altro pubblico ufficiale.

Gli strumenti di sottoscrizione elettronica assumono un autonomo rilievo anche nell'attività dell'amministrazione, sia sul fronte interno sia nel rapporto con l'utenza.

Riguardo all'attività delle amministrazioni, l'art. 23-ter stabilisce che i documenti costituenti atti amministrativi, con rilevanza interna al procedimento amministrativo, sottoscritti con firma elettronica avanzata, fanno piena prova fino a querela di falso.

Nel rapporto delle Amministrazioni con l'utenza la firma digitale del pubblico ufficiale, oltre ad integrare un requisito necessario di forma (la sottoscrizione del pubblico ufficiale che redige l'atto) integra e sostituisce (art. 24 CAD) l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

Riferimenti Normativi	*D. Lgs. n. 82/2005: artt. 1, 24, 25, 26, 27, 28, 29, 30, 31, 32, 32-bis, 33, 34, 35, 36, 37, 38, 39*
Regole tecniche e provvedimenti attuativi	- DPCM 22 febbraio 2013 (Regole tecniche firma digitale) - DPCM 10 febbraio 2010 (Autocertificazione dispositivi automatici di firma) - DPCM 19 luglio 2012 - Decreto sui dispositivi automatici di firma
Tag	*Strumenti, Diritti digitali, Organizzazione, Sicurezza*
Voci di glossario	*Certificati elettronici - Certificato qualificato - Certificatore accreditato Chiavi crittografiche – Chiave privata – Chiave pubblica - Firma elettronica – Firma elettronica avanzata – Firma elettronica qualificata – Firma digitale*