La firma digitale nel nuovo CAD: un pasticcio

di *Pierluigi Ridolfi*[1]

Con l'articolo 33 della Legge 18 giugno 2009, n. 69, il Governo è stato delegato ad aggiornare il Codice dell'amministrazione digitale (CAD: Dlgs. 82/05), seguendo alcuni specifici criteri, tra i quali "la modifica della normativa in materia di firma digitale al fine di semplificarne l'adozione e l'uso da parte della pubblica amministrazione, dei cittadini e delle imprese, garantendo livelli di sicurezza non inferiori agli attuali".
Questo "criterio" giunse del tutto inaspettato in quanto non si sentiva alcuna esigenza di modificare la norma preesistente, chiara, di uso semplice e ampiamente collaudata da milioni di utilizzatori.
Ufficiosamente si disse che occorreva adeguarsi compiutamente alla Direttiva europea del 1999 sulle firme elettroniche, se non altro nella terminologia: ma questo nulla ha a che vedere con la "semplificazione dell'uso" della firma digitale.

Il risultato è stato il Decreto legislativo 30 dicembre 2010, n. 235, che stabilisce le modifiche da apportare al CAD, tra le quali vi sono quelle relative alla firma digitale.

Per comprendere la portata di queste modifiche occorre fare un po' di storia.

La Direttiva europea del 1999 distingue la "firma elettronica"dalla "firma elettronica avanzata", definendole in questo modo:

1. "firma elettronica", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati come metodo di identificazione;
2. "firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:
   a. essere connessa in maniera unica al firmatario;
   b. essere idonea ad identificare il firmatario;
   c. essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
   d. essere collegata ai dati cui si riferisce in modo da consentire di rilevare se i dati sono cambiati.

La Direttiva poi distingue il "certificato" dal "certificato qualificato", definendoli in questo modo:

1. "certificato", un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona;
2. "certificato qualificato", un certificato contenente alcune specifiche informazioni e rilasciato da un prestatore di servizi che offra particolari garanzie, dettagliate negli allegati alla Direttiva stessa.

È anche previsto l'istituto dell' "accreditamento facoltativo", riservato a quei prestatori di servizi che si adeguano a determinati obblighi stabiliti da un apposito organismo. È consentito che, in ambito nazionale, vengano richiesti, per l'uso delle firme elettroniche nel settore pubblico, requisiti supplementari per i prestatori che operano in quel particolare mercato.

[1] Università di Bologna, già Componente del Collegio del Cnipa e Presidente della Commissione interministeriale sulla dematerializzazione. L'articolo è stato pubblicato sulla rivista IGED di gennaio 2011.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

Sono anche definite le condizioni affinché un dispositivo di firma sia considerato sicuro.

Gli effetti giuridici delle firme elettroniche sono indicati nell'articolo 5 della Direttiva:

1. se la firma è avanzata ed è basata su un certificato qualificato ed è stata creata mediante un dispositivo sicuro di firma, essa possiede i requisiti legali in relazione ai dati ai quali si riferisce, così come una firma autografa li possiede per i dati cartacei, e può essere ammessa come prova in giudizio;
2. tutti gli altri tipi di firma non possono essere dichiarati inammissibili in giudizio per il solo fatto che non appartengono alla prima categoria.

Pertanto, a seguito di questa distinzione, l'interpretazione giuridica che ne viene data è la seguente: se un documento firmato con le modalità del punto 1) viene portato in giudizio il giudice ne deve obbligatoriamente tenere conto; in tutti gli altri casi la sua l'ammissibilità è a discrezione del giudice.

Si noti che la firma avanzata "semplice", cioè senza certificato qualificato e creata da un dispositivo non sicuro di firma, NON ha le caratteristiche per essere ammessa come prova in giudizio.

Le norme sulla firma digitale, che era già stata da tempo disciplinata in Italia dal DPR 513/97 e successivamente dal DPR 445/00, per effetto del recepimento della Direttiva europea sopra citata, furono modificate con il Dlgs. 10/02 e ancora con il DPR 137/03. Successivamente, il sistema delle firme elettroniche è stato interamente rivisto nell'ambito del CAD che ha introdotto tre tipi di firma, così definiti:

1. "firma elettronica": l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
2. "firma elettronica qualificata": la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
3. "firma digitale": un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La novità maggiore sta nella scomparsa della firma avanzata "semplice" e dall'introduzione del nuovo tipo di firma denominato "firma qualificata", che coincide con la firma avanzata, come definita dalla Direttiva, dotata però di certificato qualificato e generata mediante un dispositivo sicuro. È questo il tipo firma che ha valenza legale "forte", cioè, che può essere portata in giudizio.

Questa soluzione ha il pregio della chiarezza, ma dà l'impressione di aver tolto del tutto dal sistema delle firme quella "avanzata", il che non è completamente vero.
Infatti, un caso reale di applicazione della firma avanzata è previsto dal DPR 68/05, istitutivo della Posta Elettronica Certificata (PEC), che richiede che le varie ricevute generate dal sistema siano firmate dal gestore con firma avanzata. Ci si poteva aspettare la necessità di una firma digitale, ma

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

in questo specifico caso i due tipi di firma nella sostanza coincidono, in quanto le procedure di selezione dei gestori sono restrittive al pari di quelle dei certificatori di firma digitale e, da un punto di vista tecnico, i dispositivi utilizzati dai gestori per le firme sono di tipo automatico e considerati a tutti gli effetti sicuri. C'è poi un motivo storico: il DPR sulla PEC è stato pubblicato prima del Dlgs. del CAD, quando era ancora in vigore integralmente il DPR 445/00. Si noti inoltre che il CAD non ha abrogato il DPR istitutivo della PEC.
Una secondo caso di applicazione della firma avanzata si ha quando il mittente utilizza uno dei sistemi di firma liberamente scaricabili dalla rete (molto diffuso è quello noto con la sigla PGP), che sono tecnicamente simili a quelli alla base della firma qualificata, ma con un certificato "fatto in casa" (nel quale il mittente certifica se stesso, allegando la propria chiave pubblica) e con il programma di generazione della firma contenuto nel proprio PC, che per definizione non si può considerare un dispositivo sicuro.

La firma digitale, come entità giuridica autonoma, di per sé non sarebbe necessaria, ma è stata introdotta dal CAD per uniformare la terminologia alle preesistenti norme: essa non è altro che una firma qualificata che utilizza un particolare sistema crittografico, quello delle due chiavi, una pubblica e l'altra privata.

Questa era la situazione fino all'avvento delle modifiche apportate al Codice dal Dlgs. 235/10, che, in base alla Legge delega, avrebbe dovuto semplificare la situazione. Invece di semplificare, però, il Dlgs. sopra citato reintroduce la firma avanzata e porta a quattro i tipi di firma elettronica. Questa sono le nuove definizioni:

1) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
2) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico, che consentono l'identificazione del firmatario del documento, che garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, e che sono collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
3) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
4) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

In sintesi: le definizioni 1) e 2) ricalcano quelle della Direttiva; lo stesso dicasi per la 3), che assicura un particolare valore giuridico. La 4) specifica il metodo crittografico utilizzato che, si ribadisce, deve essere uno di quelli basato sulle due chiavi, ma toglie il vincolo chiave del dispositivo sicuro di firma. Questa esclusione è sconvolgente e incomprensibile. Che si tratti un banale errore? Sono propenso a pensare di sì. Infatti, nella penultima bozza del provvedimento (come è noto, questo Decreto ha subito una ventina di rielaborazioni diverse prima di arrivare al testo definitivo) la firma digitale figurava – correttamente – come un caso particolare di firma qualificata. Pertanto, il requisito del dispositivo sicuro per la firma digitale risulta implicitamente in quanto esso è richiesto nella firma qualificata. Poi, nella definizione presente nell'ultima bozza si è

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

cambiato “qualificata” in “avanzata” (ma perché?), lasciando inalterato il resto. Così è sparito, per la firma digitale, il requisito del dispositivo sicuro.

Si è detto che la reintroduzione della firma avanzata è dovuta alla necessità di adeguarsi, almeno in termini terminologici, alla Direttiva europea. Ma corre anche voce che questa reintroduzione sia una specie di apertura in futuro a tecnologie crittografiche di tipo biometrico. Quest’ipotesi solleva però molte perplessità tecniche, in quanto i metodi biometrici possono fornire informazioni sull’identità del firmatario, ma non sui dati del documento (come richiede la Direttiva).

Fin qui, comunque, poco male (a parte la scomparsa del dispositivo sicuro di firma nella firma digitale): purtroppo, le cose si sono complicate negli articoli che disciplinano il valore giuridico dei vari tipi di firma.

Innanzi tutto è stato aggiunto all’articolo 20, relativo al documento informatico, il nuovo comma 1-bis che così recita:

“L’idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall’articolo 21”.

Sfugge il razionale di questo comma, che sembra di una totale ovvietà, in quanto non può che riferirsi a documenti non firmati (poiché quelli firmati sono disciplinati dall’articolo 21). È evidente che la valutazione in giudizio di qualunque documento non firmato è a totale discrezione del giudice: non sembra proprio che occorra una norma giuridica per stabile ciò.

Per quanto poi riguarda i documenti firmati, l’introduzione della nuova categoria della firma avanzata ha spinto il legislatore a fare un passo temerario. E qui la “colpa” non è negli uffici del Ministro, ma nella Commissione parlamentare che nel licenziare lo schema di Decreto ha formulato anche la seguente considerazione:

“6) all’articolo 1, comma 1, lettera *q*-bis) del CAD è stata introdotta, in modo condivisibile e nella prospettiva di adeguare l’ordinamento nazionale a quello comunitario che già la prevede, la nuova definizione di firma elettronica avanzata quale *genus* di firma elettronica sicura comprendente la firma elettronica qualificata e la firma digitale. Conseguentemente, per completare il coordinamento, all’articolo 1, comma 1, lettera *s)* del CAD, andrebbero sostituite, nella definizione di firma digitale, le parole: *“firma elettronica qualificata”* con le seguenti: *”firma elettronica avanzata”*. Nella medesima prospettiva, appare necessario modificare anche l’articolo 21 del CAD, in materia di efficacia sostanziale e probatoria del documento informatico sottoscritto con firma elettronica. In particolare, si suggerisce, sempre in conformità alla disciplina comunitaria, che la firma elettronica avanzata, quale *genus* delle firme elettroniche dotate di maggiore sicurezza, mutui - anche nel diritto interno - la stessa disciplina generale delle altre firme **“**sicure**”,** quali quelle qualificate e digitale. In tal modo anche al documento informatico sottoscritto con firma elettronica avanzata, va riconosciuta l’efficacia probatoria della scrittura privata ai sensi dell’articolo 2702 del codice civile”.

Riesce difficile capire che cosa ha ispirato il relatore a scrivere questa nota che contiene alcuni errori clamorosi. Infatti, non è vero che la firma elettronica avanzata abbia il genus di firma sicura, prima di tutto perché la firma sicura non esiste, poi perché la Direttiva europea dice esattamente il contrario, e cioè che la firma avanzata deve essere accettata in giudizio (in Italia v. art. 2702 CC)

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

solo se il certificato è qualificato e se la firma è stata ottenuta con un dispositivo sicuro di firma, cioè quando si tratta di firma qualificata.
Pertanto, l'affermazione che la firma avanzata "semplice" possa avere gli stessi effetti giuridici della firma qualificata (e di conseguenza di quella digitale "vecchia maniera", cioè realizzata con dispositivo sicuro), non trova appoggio alcuno nella Direttiva, anzi ne è palesemente in contrasto.

Comunque, per effetto di questa considerazione della Commissione, che il Governo difficilmente poteva ignorare, è stato modificato il testo del Dlgs., per cui, ad esempio, il comma 2 dell'articolo 21 (Documento informatico sottoscritto con firma elettronica), così recita:

"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento ha l'efficacia prevista dall'articolo 2702 del Codice civile".

Che confusione! La differenza fondamentale tra la firma avanzata e quella qualificata è che la seconda dà garanzie e la prima no. Per cui non potranno esistere regole tecniche in grado di garantire alcunché in merito alla firma avanzata generica.

Un'ulteriore considerazione: se la firma avanzata e la firma digitale hanno la stessa valenza giuridica, che ci stanno fare i "certificatori" che per ottenere questa qualifica hanno dovuto affrontare una severissima selezione?

Infine, dato e non concesso che le considerazioni precedenti siano errate, sfugge il "valore aggiunto", agli effetti di una maggiore efficienza, di questa novità (il valore giuridico pesante dato alla firma avanzata), peraltro ampiamente enfatizzata con grande risalto nel sito del Ministro.

A mio parere, l'intera impostazione della normativa sulle firme elettroniche, a partire dalla Direttiva, è basata sul presupposto della "neutralità tecnologica": ne è nato un sistema troppo "teorico". In realtà, io penso che si dovrebbe ripensare l'intera materia sulla base delle seguenti considerazioni tecniche:

1. l'unico sistema crittografico esistente per ottenere quanto previsto dalla definizione di "firma avanzata" è quello delle due chiavi;
2. qualunque sia il metodo matematico alla base di questo sistema[2], è prevista la presenza, accanto alla firma, di un "certificato" elettronico, rilasciato da un apposito ente, contenente i dati necessari per la decifrazione della firma stessa e l'identificazione del firmatario;
3. il "valore" della firma è legato all'attendibilità di chi rilascia il certificato, al tipo di dispositivo di firma utilizzato e a come sono state generate le chiavi.

Di conseguenza:

1. non può esistere nessun tipo di firma "qualificata" che non sia del tipo "digitale", la quale sola, pertanto, ha una valenza giuridica "forte";

[2] Attualmente il metodo matematico di crittografia di gran lungo più usato – per altro l'unico ammesso dalle regole tecniche in vigore in Italia – è quello noto con la sigla RSA, basato su alcune proprietà dei numeri primi; in prospettiva è ammesso anche un altro metodo, basato su alcune proprietà delle curve ellittiche.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

2. la firma avanzata ”semplice” può essere tecnicamente simile a quella digitale, ma con un certificato, una generazione delle chiavi e un dispositivo di firma “fatti in casa”, come è il caso, già accennato, della soluzione nota con la sigla PGP, che potrebbe benissimo essere utilizzato all’interno delle singole amministrazioni, come previsto dal comma 2 dell’articolo 34 del CAD.

Su questa strada si poteva lavorare per semplificare regole e applicazioni: ma nulla del genere è stato fatto.
In conclusione, il mandato dato al Governo con la Legge 69/09 era quello di semplificare le norme sulla firma digitale. Il risultato è sotto gli occhi: era difficile, ma si è riusciti a complicarle.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it