

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO

Problematiche

di formazione e probatorie

Prima di esaminare il tema oggetto della presente relazione, occorrerà fare alcune brevissime puntualizzazioni, atteso che le espressioni “firma elettronica” (meglio: “firme elettroniche”) e “firma digitale” non sono sinonimi e la differenza non è solo terminologica.

Quando si parla di **firma elettronica** s’impiega un’espressione di carattere generale, posto che esistono molti tipi di firma elettronica, tutte sostanzialmente tesi ad attribuire ad un messaggio digitale le funzioni proprie della sottoscrizione autografa.

I vari tipi potranno essere distinti per esempio in base al metodo utilizzato: tra i metodi d’autenticazione delle firme ricordiamo quelli legati ad una conoscenza propria dell’utilizzatore (numero di codice), alle sue caratteristiche fisiche (l’impronta della retina), al possesso di un oggetto (tessera magnetica).

In ogni caso, l'art. 1 del DPR n. 445\2000 co I lett. "cc", come modificato dall'art. 2 del DLGS 10\2002, qualifica come tale "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo d'autenticazione informatica".

Si parlerà poi di "**firma elettronica avanzata**" quando questa è "ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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" (v. art. 1 cit., co. I lett. "dd").

La **firma digitale** è invece una particolare specie di firma elettronica, quella che utilizza il sistema di crittografia a chiave pubblica o asimmetrica (v. art. 1 co. I lett. "n" DPR n. 445\2000 – come modificato dall'art. 2 Dlgs 10\2002: "firma digitale è un particolare tipo di firma elettronica qualificata, basata su di un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, 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...").

Altro concetto fondamentale è quello del **certificatore**, definito dall'art. 1 DPR cit. come il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. Si noti che oggi, dopo la direttiva europea 1999\93\CE ed il recepimento della stessa nel nostro ordinamento ad opera del Dlgs. n. 10\2002 (v. oltre), l'attività di certificazione è libera e non necessita d'autorizzazione preventiva, così innovandosi rispetto al rigoroso sistema delineato dal legislatore italiano con i DPR n. 513\1997 e 445\2000, che prevedevano un unico certificato normativamente disciplinato e un'unica figura di certificatore, inserita in un apposito elenco pubblico dopo aver dimostrato di possedere vari requisiti tecnici, giuridici e morali (v. art. 27 DPR n. 445\2000).

I **certificati elettronici** sono, sempre secondo la stessa disposizione di legge, gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (nell'art. 1 in esame si possono poi individuare vari tipi di certificato e di certificatori, cui si può fare integrale rinvio).

Passando al tema che ci occupa, il riferimento normativo principale è costituito dall'**art. 10 DPR 445\2000**, come novellato dall'art. 6 DLGS 10\2002.

Tale norma è stata come sopra modificata per adeguare l'ordinamento italiano alla direttiva n. 1999\93\CE del Parlamento Europeo e del Consiglio.

Con tale direttiva, come s'è visto, si voleva liberalizzare il mercato dei certificatori e la circolazione delle firme elettroniche e, pertanto, si è reso necessario operare con la citata novella.

Il I comma dell'art. 10 cit. prevede che “il documento informatico ha l'efficacia probatoria prevista dall'art. 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate”.

Con l'ultimo inciso, quindi, si riporta la medesima formulazione utilizzata dal CC, con l'ovvia, ulteriore aggiunta che tale efficacia è subordinata al fatto che “colui contro il quale” il documento è prodotto “non ne disconosce la conformità ai fatti o alle cose medesime” (occorrerà pertanto, secondo la costante giurisprudenza di legittimità – v. p.es., Cass. Civ., 3.7.2001 n. 8998 – una contestazione esplicita, processualmente equiparabile ad un'ordinaria eccezione in senso lato, e in tal caso il giudice potrà accertare la contestata conformità con ogni mezzo di prova, ivi incluse le presunzioni – v. Cass. Civ., 6.9.2001 n. 11445).

Ovviamente, il documento informatico di cui sopra è un documento non sottoscritto né digitalmente né in altra maniera. Come tale, ci si rende conto che la norma in esame si applicherà alla gran parte dei

documenti che transitano nella rete (diverso è il caso, affrontato dalla recente Cass. Civ. Sez. Lavoro, 16.2.2004 n. 2912, che ha ritenuto non utilizzabile a fini probatori una copia di “pagina Web” trasferita su supporto cartaceo, che non risulti esser stata raccolta con garanzia di rispondenza all’originale e di riferibilità ad un ben individuato momento).

In ogni caso, nulla dice il legislatore circa l’integrità del documento, anche se spesso ciò che è importante accertare non è la paternità, ma l’assenza di modifiche o falsificazioni. Benché probabilmente ci sia la possibilità tecnica di delineare vari livelli di sicurezza, in assenza di disposizioni specifiche, tale possibilità potrà esser prospettata dalla parte che intende avvalersi del documento al giudice, onde contribuire a formare il suo libero apprezzamento della prova, fermo restando che ogni difesa di controparte dovrà comunque basarsi sul citato disconoscimento.

Nella attesa del cd. processo informatico, il problema pratico è quello della consultabilità di siffatto documento: perché non sia altrimenti sempre necessario un “computer” occorrerà trasferire il suo contenuto su carta. Onde risolvere tale problema, il giudice potrà disporre nei casi più semplici (sostanzialmente risolvendosi in una trascrizione) la riproduzione ex art. 261 CPC del documento informatico su carta, mentre, per i casi più complessi (si pensi a

documenti danneggiati o parzialmente crittografati), si potrà ricorrere ad una CTU e/o all'ispezione di cui all'art. 259 CPC (a quest'ultimo istituto si dovrà ricorrere, con o senza l'assistenza del CTU, quando il contenuto del documento non sia riproducibile su carta – si pensi a brani musicali o a sequenze filmate).

Passando al **II comma dell'art. 10 cit.**, con esso si stabilisce che “il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare”.

Per un attimo richiamando quanto sopra detto in tema di firma elettronica, la norma in esame non attribuisce al documento in esame una precisa efficacia probatoria: non avremo quindi una prova legale, ma una prova soggetta alla libera valutazione del giudice ex art. 116 CPC. Il “peso” probatorio di tale documento non sarà percepibile prima del processo, ma diverrà evidente solo in esito alla suddetta valutazione e, quindi, al processo.

L'incertezza aumenta sol che si consideri la citata genericità definitoria del legislatore in tema di firma elettronica e la

conseguente possibilità di configurare svariati tipi di tale firma (più sicuri o meno sicuri a seconda del tipo d'autenticazione prescelto). Proprio per tali motivi appare del tutto condivisibile la scelta di affidare al giudice la decisione da adottare caso per caso: con la norma in questione, peraltro, si è definitivamente e pienamente legalizzato l'uso di siffatte prove, così per esempio potendosi provare una transazione economica attraverso la traccia elettronica della carta di credito. Del resto, così facendo si è data piena attuazione alla direttiva europea 1999\93\CE che prevedeva per gli stati membri l'impossibilità di considerare inammissibile o inefficace la firma elettronica per il solo fatto della sua "elettronicità" o dell'assenza di una sua certificazione o creazione in termini di sicurezza.

Bisogna comunque rilevare che la prova in esame non è considerata come scrittura privata ex art. 2702 CC, pur soddisfacendo "il requisito legale della prova scritta". Ne conseguirà che gli atti o i contratti per la cui validità si richiede la forma scritta potranno esser contenuti nei documenti informatici con firma elettronica, ma la loro efficacia probatoria non sarà quella della scrittura privata, rimanendo affidata al giudice ex art. 116 CPC. Ancora una volta, però, attesa la possibilità di adottare legittimamente svariati tipi di firma elettronica, la altrimenti poco comprensibile separazione tra validità ed efficacia probatoria del documento con firma elettronica appare comunque

giustificata, altrimenti potendosi attribuire, in nome di formali esigenze concettuali, la medesima, rilevante efficacia probatoria a più o meno sicuri metodi d'autenticazione.

Più complesso è il successivo **comma III dell'art. 10 cit.**.

In esso si parla di “firma digitale”, di “firma elettronica avanzata”, di “certificato qualificato”, di un “dispositivo per la creazione di una firma sicura” (per la nozione relativa a queste due ultime definizioni, v. art. 1 co. I lett. “aa” e “ii” DPR n. 445\2000).

Si delineano pertanto due tipi di documento informatico (uno sottoscritto con firma digitale ed uno sottoscritto con l'utilizzo degli altri tre strumenti sopra elencati), ambedue peraltro dotati dell'efficacia di piena prova, fino a querela di falso (verosimilmente, l'oggetto di tale giudizio si incentrerà in genere sull'uso abusivo o illecito di una chiave privata altrui). L'efficacia sarà pertanto quella della scrittura privata riconosciuta o non disconosciuta ex art. 2702 CC.

Quanto alla **firma digitale**, essa era già conosciuta dall'ordinamento previgente (v. DPR n. 513\1997 e 445\2000 ante novella), ma la norma in esame ha il pregio di dirimere una controversia sorta per l'appunto in tale periodo: ferma restando per documento sottoscritto con la firma digitale l'efficacia di cui all'art. 2702 CC, si discuteva in dottrina se tale efficacia fosse già in prima battuta fino a querela di

falso o se, invece, per arrivare a tale risultato si dovesse autenticare la sottoscrizione o la si dovesse riconoscere o non disconoscere.

Oggi, pertanto, tale tipo di documento non potrà più esser disconosciuto ex art. 215 CPC, ma potrà esser solamente impugnato con la querela di falso.

Sotto un profilo tecnico, il dispositivo di autenticazione a chiavi asimmetriche riesce a garantire non solo la provenienza della dichiarazione informatica, ma anche l'integrità del documento che la contiene, perché, se si modifica un suo elemento anche minimo dopo la cifratura con la chiave privata, tale documento non viene più riconosciuto dalla chiave pubblica nell'ambito della procedura di verifica.

Sempre in tema di firma digitale, ci si chiede come coordinare il parimenti vigente disposto del successivo art. 24 ("si ha per riconosciuta, ai sensi dell'art. 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato") con la disposizione in esame, che considera la firma digitale già munita, in sé e per sé, dell'efficacia di prova legale.

Secondo una parte della dottrina si sarebbe verificata un'abrogazione tacita dell'art. 24 da parte dell'art. 6 DLGS 10\2002 (che ha per l'appunto modificato l'art. 10 in esame), mentre secondo altri le due

norme possono ancora coesistere (infatti, in caso di firma autenticata – art. 24 - l'oggetto della querela di falso verterà unicamente sulla falsità della dichiarazione del pubblico ufficiale, avendo quest'ultimo certificato la coincidenza tra utilizzatore e titolare della chiave privata; nei restanti casi – art. 10 -, tale oggetto verterà sull'abusivo o fraudolento uso della chiave privata).

Quanto alla **firma elettronica avanzata**, il livello e lo “standard” di sicurezza da cui derivano l'efficacia probatoria privilegiata del documento non sono individuati con precisione dal punto di vista tecnico, limitandosi il legislatore a prevedere tre requisiti minimi necessari per la sicurezza delle firme elettroniche, con chiaro utilizzo e attuazione del principio di “neutralità tecnologica”, a cui si è sempre ispirata la legislazione comunitaria.

Ovviamente, a tale ampia e pragmatica apertura tecnologica (verosimilmente ispirata da criteri economici e imprenditoriali propri di un regime di libera concorrenza e di libero mercato), dovrà fare da contraltare (anche alla luce della relevantissima efficacia probatoria attribuita al documento in esame) un quanto mai rigoroso e severo controllo su quel terzo che contribuisce a garantire, attraverso il rilascio del certificato qualificato, l'autenticità della sottoscrizione, a pena di rendere meno sicuri i traffici commerciali e la circolazione dei beni (v. artt. 26, 27 e 29 DPR 445\2000 testo vigente).

Anche per la firma elettronica avanzata, come per la firma digitale, la garanzia di autenticità dovrebbe valere sia per la provenienza che per l'integrità del documento, altrimenti nessun senso avendo l'inciso contenuto nella norma definitoria di cui all'art. 1 co I lett. "dd" già citato ("... consentire di rilevare se i dati stessi siano stati successivamente modificati").

Abbiamo quindi visto che i due tipi di sottoscrizione esaminati nel comma III garantiscono tanto la provenienza quanto l'integrità del documento informatico, epperò la "piena prova, fino a querela di falso" è in esso limitata alla sola "provenienza delle dichiarazioni di chi l'ha sottoscritto".

Orbene, attesa la non contestabilità di quanto prima rilevato sotto l'aspetto tecnico dei due tipi di firma, appare possibile interpretare estensivamente la disposizione in questione, nel senso di poter estendere la suddetta efficacia probatoria anche all'integrità del documento.

La validità della certificazione apposta sia in caso di firma digitale che in caso di firma elettronica avanzata, peraltro, avrà un termine di scadenza stabilito dal certificatore (v. art. 4 co. VII allegato tecnico al DPCM 8.2.1999 – il termine massimo, stabilito in tre anni dall'art. 22 co I lett. "f" del DPR 445\2000, non esiste più, a seguito della modifica operata dall'art. 8 DPR 7.4.2003 n. 137).

Non resta che esaminare il **IV comma dell'art. 10 cit.**

Il testo di tale norma, in sostanza riprodotto il dettato dell'art. 5 co. II della direttiva europea, comporta due conseguenze.

La prima, secondo cui inevitabilmente deve riconoscersi dignità di prova ai documenti informatici ivi descritti, fermo restando che gli stessi dovranno esser valutati dal giudice ex art. 116 CPC e potranno esser disconosciuti dalla controparte secondo le vigenti regole procedurali ex artt. 214 e ss CPC, con il conseguente, eventuale innesto, nella causa in corso, del procedimento di verifica ex art. 216 CPC.

La seconda, in base alla quale si può ipotizzare la presenza e la diffusione di sistemi di certificazione e di sottoscrizioni privi dell'efficacia privilegiata propria delle firme di cui ai precedenti commi, ma purtuttavia legittimi e qualificati, sia pure nei limiti già visti, come prove.

Rimane da comprendere l'utilità di siffatta norma, apparendo la stessa assorbita e ricompresa nel più ampio disposto del primo e del secondo dell'art. 10 (le differenze – esigue per la verità - sembrano consistere nel fatto che nel primo comma ci si muove nell'ambito dell'efficacia probatoria propria dell'art. 2712 CC, nel secondo e nel quarto nell'ambito dell'efficacia propria degli artt. 116 e 214 e ss CPC, evidenziandosi peraltro che nel secondo non v'è un

certificatore, mentre nel quarto c'è un certificatore privo degli attributi previsti dalla legge per ottenere l'efficacia della piena prova).

Per concludere, qualche brevissima considerazione sulla **data del documento informatico**, atteso che in tale materia è immediatamente percepibile la novità delle norme in tema di documento informatico rispetto a quella contenuta nell'art. 2704 CC. L'art. 14 co II del DPR 445\2000 prevede, infatti, che “la data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico ed alle regole tecniche di cui agli articoli 8, comma 2, e 9, comma 4, sono opponibili ai terzi”.

L'attribuzione della data avviene attraverso la cd. procedura di validazione, definita dall'art. 22 lett. “g” del DPR 445\2000 come “il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi”: si tratta in sostanza di una dichiarazione proveniente da un certificatore (ente abilitato a fornire un servizio di validazione temporale) chiamata “marca temporale”, modellata secondo il già noto sistema delle chiavi asimmetriche.

Il documento, quindi, conterrà la sottoscrizione di chi ha apposto la marca temporale (tale strumento tecnico è fra l'altro congegnato in

modo tale da non consentire al certificatore di conoscere il contenuto del documento), sottoscrizione che si potrà aggiungere a quella di chi ha certificato la firma digitale.

Anche la validità di tale certificazione temporale, peraltro, avrà il termine di scadenza stabilito dal certificatore (v. art. 4 co. VII allegato tecnico al DPCM 8.2.1999, già sopra citato).

Orbene, per prolungare la suddetta validità o, meglio efficacia probatoria (e quanto si dirà vale anche per le certificazioni in tema di firma digitale ed elettronica avanzata), in base allo schema regolamentare previsto dall'art. 60 dell'allegato tecnico al DPCM cit., l'interessato dovrà, prima della scadenza, procedere alla (nuova) validazione temporale del documento il cui certificato di firma digitale stia scadendo (si prorogherà così la sua efficacia privilegiata per un periodo uguale a quello della validazione temporale effettuata, salvo nuovi, successivi rinnovi) o ottenere una nuova marca temporale prima della scadenza di quella già esistente (la data del documento continuerà così ad esser opponibile ai terzi): ovviamente, potendo coesistere sul medesimo documento i due tipi di certificazione, il rinnovo aggiornerà l'efficacia probatoria del documento sotto il duplice profilo certificatorio.

La parte dovrà quindi preoccuparsi di tener d'occhio le scadenze dei termini fissati dal certificatore, in caso contrario residuando pel

documento l'efficacia probatoria prevista, a seconda dei casi, dai
commi I, II o IV dell'art. 10 DPR 445\2000.

Verona, 7.5.2004.

(dott. Ernesto D'Amico)

Giudice del Tribunale di Verona