LA FIRMA DIGITALE E LA POSTA ELETTRONICA CERTIFICATA

Dario Obizzi

Premessa

L'utilizzo sempre più diffuso delle nuove tecnologie e quindi di elaboratori e di sistemi informatici e telematici ha creato profondi, e non sempre ben sfruttati e compresi, cambiamenti nella vita quotidiana e professionale.

La facilità di comunicare e di mettersi in contatto con altri soggetti, inviando fax, e-mail, sms, mms, file allegati e quant'altro, ha indubbiamente consentito un miglioramento delle relazioni interpersonali ed economiche ma, al contempo, ha posto una serie di nuove problematiche.

In campo giuridico si è posta da subito la questione relativa al riconoscimento ed al valore da attribuire alle informazioni create, generate, trasmesse o comunque prodotte da sistemi informatici e telematici. Tali informazioni, contenute in un file o in un'e-mail e che possono apparire all'utente come un testo, una fotografia, etc.., sono equivalenti ed hanno lo stesso valore di quelle informazioni contenute in un documento cartaceo o in una fotografia analogica? La risposta non è stata semplice ed è giunta solo dopo un cammino legislativo abbastanza lungo. In Italia, infatti, già dagli anni ottanta si erano susseguite delle norme che avevano disciplinato l'uso di strumenti elettronici ed i requisiti per attribuire ai documenti da loro generati o trasmessi efficacia e valenza probatoria (si pensi all'uso del fax nei rapporti tra avvocati[1] oppure all'introduzione dell'art. 491-bis del codice penale in tema di documento informatico[2]), ma nessuna aveva preso una posizione estremamente precisa sul punto.

La disciplina legislativa

Solo con l'art. 15 della Legge n. 59 del 1997 (cd. legge Bassanini) veniva affrontata di petto la questione, stabilendo che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o 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". Successivamente il D.P.R. 513/97 (ora abrogato) ed il D.P.R. 445/2000 (Testo Unico in materia di documentazione amministrativa) contenevano la definizione di "documento informatico" quale rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Con tali interventi legislativi il nostro ordinamento, quindi, riconosceva espressamente e pienamente validità e rilevanza al documento informatico quale prodotto di un elaboratore o apparato similare. Tuttavia restava ancora irrisolta una questione di primaria importanza: la possibilità di risalire con certezza alla paternità del documento informatico (si pensi, ad esempio, ad una e-mail). La soluzione veniva individuata nell'utilizzo (rectius, nell'apposizione o associazione) della firma digitale, quale sistema, simile alla firma autografa su carta, di autenticazione dei documenti informatici.

La firma digitale

La firma digitale, *species* di quello che oggi è il *genus* firma elettronica qualificata, si basa sulla tecnologia della crittografia a chiavi asimmetriche o a chiave pubblica. Ogni utente dispone di una coppia di chiavi: una chiave privata, da non svelare a nessuno e con cui firmare il documento informatico, ed una chiave pubblica, che gli altri utenti utilizzano per decodificare la firma e constatarne quindi l'autenticità. Questa procedura serve a garantire due cose: l'autenticità (certezza del sottoscrittore) e l'integrità (non modificabilità) del documento. Per ottenere la segretezza del documento, si deve utilizzare il procedimento inverso: apponendo la chiave pubblica del titolare della chiave privata si ottiene la codifica del messaggio; solo il titolare, tramite la propria chiave privata, sarà in grado di decodificare il messaggio.

La procedura di apposizione della firma digitale, più dettagliatamente, consiste in questo: tramite una funzione di *hash*, che ha lo scopo di trasformare un testo di qualsiasi lunghezza in una stringa di lunghezza fissa[3], si ricava l'impronta digitale del documento e, tramite la chiave privata, si codifica l'impronta così ricavata. Questo comporta un notevole vantaggio in quanto la codifica riguarda solo una piccola stringa e non

l'intero messaggio o documento che, in alcuni casi, può avere dimensioni molto grandi. La firma viene quindi allegata al documento e chiunque, utilizzando la chiave pubblica del firmatario, decodifica l'impronta digitale e confronta la stringa così ottenuta con quella che ottiene egli stesso applicando la funzione di *hash*.

Naturalmente tali operazioni vengono eseguite in automatico da appositi software. Qualora i risultati combacino, l'autenticità e l'integrità del documento sono garantite.

Per ottenere la firma digitale bisogna rivolgersi ad un soggetto, denominato ente certificatore (che può essere accreditato o notificato dal CNIPA), che, vista la delicatezza del ruolo, deve assicurare solidità e sicurezza dei sistemi operativi, della struttura organizzativa e finanziaria. Si tratta in sostanza di un ente terzo, neutrale e di fiducia, cui è demandato il compito di fornire il dispositivo di firma sicuro al titolare, verificare ed attestare, emettendo un apposito certificato digitale qualificato, l'identità del titolare, pubblicare sul web il certificato e la chiave pubblica per permettere a chiunque di verificare l'avvenuta certificazione. L'ente certificatore, inoltre, deve essere incluso in un elenco pubblico, consultabile sul sito del CNIPA. Tutto ciò comporta anche l'assunzione di responsabilità da parte del certificatore nei confronti di coloro che abbiano fatto affidamento sul corretto adempimento degli obblighi gravanti sullo stesso certificatore (esattezza delle informazioni necessarie alla verifica della firma, tempestiva registrazione della revoca o sospensione del certificato, etc.).

La firma digitale è quindi molto simile, ma non uguale, alla firma autografa. Mentre la sottoscrizione diventa parte integrante del documento, la firma digitale è in realtà un allegato; la verifica poi segue strade diverse in quanto la firma autografa richiede il confronto con un'altra firma (metodo non molto sicuro), mentre la firma digitale si avvale di un algoritmo e quindi di un sistema più affidabile. L'aspetto che però più distingue i due tipi di firma è quello relativo all'integrità del documento: la firma autografa non è in grado di dare certezza riguardo a eventuali

modificazioni, mentre la firma digitale si. Per converso, la firma digitale manifesta un limite molto evidente: la validità temporale limitata.

Il valore giuridico

Resta a questo punto da verificare il valore giuridico della firma digitale.
Come detto, il D.P.R. 10 novembre 1997 n. 513, emanato in attuazione dell'art. 15 della legge 15 marzo 1997, n. 59, prevedeva che il documento informatico, sottoscritto con firma digitale, avesse l'efficacia probatoria di cui all'art. 2702 c.c., riguardante, come ben noto, l'efficacia della scrittura privata.
Successivamente tale normativa era stata trasposta nel D.P.R. 28 dicembre 2000, n. 445 che, a sua volta, ha subito molteplici modifiche, dovute anche alla necessità di adattare la legislazione nazionale alla Direttiva europea 99/93. Attualmente la materia è disciplinata dal Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005 n. 82, così come modificato dal D.Lgs. 4 aprile 2006 n. 159), il quale prevede tre (rectius, due) tipi di firme elettroniche: la "firma elettronica" e la "firma elettronica qualificata". La "firma digitale" è un particolare tipo di firma elettronica qualificata. La firma elettronica cd. "semplice" è definita come un insieme di dati in forma elettronica, allegati o connessi ad altri dati, utilizzati come metodo di identificazione informatica (ad es. gli *header* dell'e-mail). La firma elettronica qualificata, invece, richiede in più un'identificazione univoca del titolare, tramite mezzi nell'esclusiva disponibilità del firmatario (quindi smart-card, token USB), e la certificazione del titolare da parte di un soggetto terzo e tramite un certificato qualificato. La firma digitale, oltre ad essere una firma qualificata, è contraddistinta dall'utilizzo della tecnologia della crittografia a chiavi asimmetriche. Ciò premesso, l'art. 20 del D.L.vo 82/05 stabilisce che l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile nel giudizio; se vi è apposta la firma digitale, il documento informatico si presume riconducibile al titolare, salvo che questi dia prova contraria (quindi vige il principio inverso rispetto alla sottoscrizione in cui la controparte deve dimostrare la

riconducibilità al firmatario), e soddisfa il requisito della forma scritta. L'art. 21 aggiunge che il documento informatico cui è apposta una firma elettronica è liberamente valutabile nel giudizio sul piano probatorio, mentre, nel caso di apposizione di firma digitale, l'efficacia è quella dell'art. 2702 c.c.

Riassumendo, il documento informatico ha validità e rilevanza nel nostro ordinamento: se è apposta una firma elettronica avrà un'efficacia probatoria da valutare caso per caso, mentre in presenza di una firma digitale il documento informatico diventa una vera e propria scrittura privata sottoscritta (salvo l'inversione dell'onere della prova per quanto riguarda il disconoscimento).

L'utilizzo della firma digitale può essere quindi il più vario: dai rapporti con le pubbliche amministrazioni (si pensi, ad esempio, al principio sancito dall'art. 3-bis della L. 241/90: per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati), alle dichiarazioni fiscali, alle transazioni finanziarie e bancarie, ai rapporti contrattuali, alla fornitura elettronica di beni e servizi, alle operazioni di identificazione e autorizzazione, etc.

La Posta Elettronica Certificata

Di pari passo con la regolamentazione della firma digitale, si è cercato di risolvere anche il problema relativo alla trasmissione del documento informatico.

Il ricorso alla posta elettronica per l'invio del messaggio informatico, infatti, si è rivelato inidoneo a garantire la provenienza del documento da parte di un soggetto determinato, l'integrità del contenuto e, soprattutto, la volontarietà dell'invio. Per ottenere gli stessi effetti prodotti da una lettera raccomandata con ricevuta di ritorno si è quindi fatto ricorso alla Posta Elettronica Certificata (PEC). Con tale sistema il mittente riceve l'attestazione, da parte del gestore della posta elettronica, dell'invio e della consegna dei documenti informatici (anche privi di firma digitale) al destinatario (rectius, al provider del destinatario). La certificazione fornita

dal gestore di PEC costituisce prova legale dell'avvenuta trasmissione di un messaggio, come accade per l'avviso di ricevimento nella raccomandata[4]. Per ottenere tale risultato è però necessario che anche il destinatario abbia un indirizzo di posta elettronica certificata; in caso contrario, l'effetto ottenuto sarà assimilabile ad una raccomandata senza ricevuta.

Il D.P.R. 11 febbraio 2005 n. 68 disciplina le modalità di utilizzo della PEC[5]: i provider della posta elettronica certificata, enti autorizzati e molto simili ai certificatori della firma digitale, appena ricevono il messaggio da inviare forniscono al mittente la ricevuta di accettazione. Subito dopo il messaggio viene inserito dal gestore in una busta di trasporto, unitamente alla relativa ricevuta fornita. La busta e la ricevuta vengono quindi sottoscritte con firma elettronica avanzata e ad ogni messaggio viene apposta una marcatura temporale (*time stamping*). La busta viene quindi inviata al destinatario: il gestore della PEC del destinatario invia al gestore del mittente una ricevuta di presa in carico ed effettua dei controlli sulla presenza di virus o altre anomalie.

Terminati tali controlli, il gestore del destinatario invia una ricevuta di avvenuta consegna che, indipendentemente dalla avvenuta lettura, certifica che il messaggio è stato consegnato nella casella di PEC del destinatario.

Qualora l'e-mail non sia consegnabile (ad es. account non più attivo), il gestore comunica al mittente nelle ventiquattro ore successive la mancata consegna.

Tale procedura di trasmissione è valida agli effetti di legge[6].

Il sistema così come è attualmente configurato e previsto presenta però due inconvenienti che ne rallentano la diffusione[7]: il primo è la conoscibilità dell'indirizzo di posta elettronica certificato del destinatario (la legge parla di indirizzo "dichiarato" o addirittura "espressamente dichiarato"[8]); il secondo è quello relativo ai costi, soprattutto se rapportato all'e-mail, quasi sempre gratuita.

[1] Si veda la Legge 7 giugno 1993, n. 183 (in Gazz. Uff., 14 giugno, n. 137). - Norme in materia di utilizzazione dei mezzi di telecomunicazione per la trasmissione degli atti

relativi a procedimenti giurisdizionali. L'art. 1 prevede che, in presenza di determinati requisiti, "la copia fotoriprodotta di un atto del processo redatto e sottoscritto da un avvocato o da un procuratore e trasmesso a distanza attraverso i mezzi di telecomunicazione ad altro avvocato [o procuratore], si considera conforme all'atto trasmesso".

[2] Secondo tale norma "per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

[3] L'hash MD5 è rappresentato come una sequenza di 32 cifre esadecimali. Il famoso incipit dell'Iliade "Cantami o diva del pelide Achille l'ira funesta" corrisponde alla seguente stringa: b4dd7f0b0ca6c25dd46cc096e45158eb. Basta cambiare una lettera "C**o**ntami o diva del pelide Achille l'ira funesta" e la stringa cambia completamente: f065b51db9c592bf6ecf66a76e39f8d0. Tale esempio è riportato su http://it.wikipedia.org/wiki/MD5

[4] L'art. 45 del Codice dell'Amministrazione Digitale è chiaro sul punto: il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

[5] Per le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica è stato emanato il D.P.C.M. - Dipartimento per l'innovazione e le Tecnologie 2 novembre 2005 (in Gazz.Uff., 15 novembre, n. 266). - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.

[6] Si veda l'art. 14 D.P.R. 445/2000 (ora abrogato) ed il D.P.R. 11 febbraio 2005 n.68 (in Gazz. Uff., 28 aprile, n. 97). - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata. Sul punto anche l'art. 48 del Codice dell'Amministrazione Digitale che riconosce alla trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, la stessa efficacia, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

[7] Si veda a tal proposito la Legge 16 gennaio 2003 n. 3 (in Suppl. ordinario n. 5 alla Gazz. Uff., 20 gennaio, n. 15). - Disposizioni ordinamentali in materia di pubblica amministrazione.
L'art 27 prevede, tra i vari obiettivi da conseguire, la diffusione dell'uso delle firme elettroniche.

[8] È previsto, ad esempio, che le imprese, nei rapporti tra loro intercorrenti, possano dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese.
Da ultimo va segnalato che la Legge 6 agosto 2008, n. 133 ha previsto espressamente all'art. 51 che le notificazioni e le comunicazioni di cui al primo comma dell'articolo 170 del codice di procedura civile, la notificazione di cui al primo comma dell'articolo 192 del codice di procedura civile e ogni altra comunicazione al consulente vengano effettuate per via telematica all'indirizzo elettronico "comunicato" ai sensi dell'articolo 7 del regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2001, n. 123