L'*E-MAIL* DIVENTA CERTIFICATA. IL VALORE PROBATORIO DELLA POSTA ELETTRONICA.

di Davide Binda
dottore in legge, studio legale e commerciale Giuliano & Di Gravio

Finalmente uno dei mezzi di comunicazione più utilizzati al mondo, semplice ed economico, ottiene le luci della ribalta in Italia ottenendo la "certificazione".

Specialmente negli ultimi anni, lo sviluppo di internet e delle nuove tecnologie in genere, ha portato a focalizzare l'attenzione su questo nuovo mezzo di comunicazione/trasmissione che con i quasi 400 milioni di lettere virtuali scambiate al giorno nel 2004, in Italia, e con una previsione di incremento del 25% per il 2005, porterà il monte complessivo delle missive scambiate nel nostro paese a quota 186 miliardi l'anno.

Una realtà che dunque, oggi più che mai, si fa forzatamente strada e che il 25 marzo 2004 ha preso le proprie mosse con l'approvazione di un regolamento da parte del Consiglio dei Ministri su proposta degli onorevoli Stanca e Gazzella. Il provvedimento colloca certamente l'Italia tra i primi paesi al mondo a dare completa validità giuridica ai documenti trasmessi via e-mail, che assurgono così a vedersi riconosciuta l'efficacia probatoria che nel nostro ordinamento veniva già riconosciuta alla raccomandata con ricevuta di ritorno. Il provvedimento inoltre si trova ad introdurre una nuova disciplina per ciò che concerne l'utilizzo della posta elettronica certificata non solo nei rapporti che cittadini ed imprese intratterranno con la Pubblica amministrazione, ma anche nelle relazioni telematiche instaurate tra uffici pubblici, come pure tra semplici privati.

Il decreto, come sottolineato durante la conferenza stampa da uno dei sui "padri", l'on Stanca, era stato licenziato dal Consiglio dei Ministri il 25 marzo scorso e, dopo essere passato al vaglio della Conferenza Unificata, del Consiglio di Stato, del Parlamento, dei Ministeri e della Commissione U.E, ha ultimato il proprio iter legislativo con la pubblicazione sulla Gazzetta Ufficiale n. 97 del 28 aprile 2005.

Occorre per onore del vero, preliminarmente sottolineare e precisare che il "documento" del quale proveremo ad individuare le generalità e del quale studieremo l'efficacia non risulta costituito dalla semplice comunicazione via e-mail, quale quella, che siamo abituati a utilizzare in veste di quotidiani utilizzatori e utenti della rete internet.

La finalità principale di detto decreto, vuole essere costituita dal riconoscimento della certificazione dell'invio e della relativa ricezione del documento in questione. Con il termine "invio" si intende la procedura attraverso la quale il mittente in seguito all'inoltro del documento riceve dal proprio gestore di posta elettronica una vera e propria ricevuta di ritorno di avvenuto invio della e-mail, ricevuta che costituisce prova legale dell'invio stesso con la possibile presenza di allegati. Nello stesso identico modo, nel momento in cui il messaggio raggiunge la casella di posta del destinatario, il server di posta di quest'ultimo inoltra al mittente la ricevuta di avvenuta (o mancata) consegna con l'esplicita indicazione di giorno e ora, il tutto indipendentemente e a prescindere dall'apertura o meno del messaggio da parte del ricevente. L'intera operazione risulta sottoscritta e validata attraverso una firma elettronica avanzata, creata in modo automatico dal sistema, firma che trova le proprie basi all'interno di un sistema di chiavi asimmetriche a coppia, una denominata "pubblica" e una "privata".[1] Mediante la ricevuta di consegna della missiva virtuale è inoltre prevista la possibilità di re-inviare al mittente l'intera copia del testo spedito.

Prima di giungere a rendere possibile questa forma di "certificazione forte" che, come vedremo in prosieguo, introduce forti novità per ciò che concerne l'interpretazione della materia nel campo dei mezzi probatori, occorre sottolineare come il decreto stesso preveda l'istituzione di un elenco ufficiale di gestori di posta elettronica certificata, qualificati e riconosciuti, presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, il quale ha tra i propri fini statutari il compito di vigilare e controllare l'operato e il rispetto della legislazione da parte dei server stessi.

Presso ogni server/gestore di posta elettronica deve necessariamente essere istituito un Log dei messaggi, un vero e proprio registro informatico all'interno del quale verranno registrate tutte le informazioni relative alle operazioni inerenti le trasmissioni effettuate con posta elettronica certificata. La possibilità di tracciare la "storia" informatica delle operazioni svolte, aventi del resto lo stesso valore giuridico delle ricevute di ritorno per quanto riguarda il servizio postale, sarà consentita per almeno 30 mesi[2], e costituirà una sorta di "rete di sicurezza" che in ogni momento permetterà di risalire allo scambio di informazioni effettuato, anche nel malaugurato caso in cui il mittente non avesse conservato la ricevuta virtuale.

[1] Il sistema si basa su un doppio sistema di codici-password, una denominata "pubblica" che viene certificata dal server e stabilita al momento dell'iscrizione al servizio, una seconda chiave detta "privata" conosciuta solo dal titolare dell'indirizzo e-mail. Il sistema adotta lo stesso procedimento di quello che occorre per cripatare i numeri di carte bancomat e di credito.

[2] Trascorsi trenta mesi il gestore/server ha la possibilità di eliminare i dati relativi alle trasmissioni.

Da sottolineare che da un punto di vista maggiormente tecnico, particolare attenzione è stata prestata alla previsione dei rischi connessi alla tecnologia *de quo*, ci riferiamo alla possibile presenza di virus informatici, programmi che lanciati sulla rete internet, "infettando" i software sono in grado di modificare, distruggere o de-settare gli applicativi con le relative documentazioni. Ricordando che stiamo parlando di comunicazioni informatiche che possiedono valore ed efficacia probatoria, si comprende immediatamente il fatto di quanto sia delicata la situazione. Per aggirare detto problema è stata prevista la realizzazione di un doppio filtro da parte dei gestori di posta (del mittente e del destinatario) i quali sono tempestivamente tenuti[3] a bloccare l'invio e la ricezione delle e-mail in caso di rilevazione della presenza di virus, con l'obbligo di segnalare detta presenza al mittente.

Giunti a questo punto, tralasciando il lato più pratico/tecnico del sistema di invio/ricezione di detta documentazione, occorre soffermarsi su quale e come si presenti il panorama legislativo in materia e soprattutto arrivare a comprendere quale sia la portata della validità legale delle e-mail informatiche.

Certamente attraverso il D.P.R in questione si vengono a delineare nuovi punti fermi e si sciolgono delicati interrogativi nati negli ultimi anni, grazie allo sviluppo e alla diffusione della tecnologia connessa a internet

Concedendoci un breve *excursus* storico, occorre rammentare che i primi passi in materia sono stati mossi con il D.P.R. n.513/1997 che nello specifico del suo articolo 8) riconoscendo, a tutti gli effetti, la validità del documento informatico, ha lasciato spazio a differenti interrogativi circa il valore probatorio di questi ultimo. Proprio in virtù di questo decreto, lo scambio di dati o la semplice registrazione su supporto informatico degli stessi, rappresenta e acquista la validità di un vero e proprio documento elettronico/informatico, documento appunto perché fornito di capacità rappresentativa.

Il problema chiave riguardante detta tecnologia, si riscontra nel nodo concernente la possibilità di una corretta attribuzione della provenienza dello stesso. Infatti la funzione probatoria che nella scrittura privata viene espletata con la sottoscrizione da parte del/degli autore/i del documento,[4] deve in questo caso essere operata attraverso la previsione di un meccanismo differentemente organizzato.

[3] Detta previsione di un sistema a doppio filtro costituisce un vero e proprio obbligo da parte dei gestori stessi, obbligo sul quale vigilerà il Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

[4] Art. 2702 c.c. Efficacia della scrittura privata. – La scrittura privata fa piena prova , fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

Prefiggendoci di intraprendere una sorta di analisi storico/materiale relativa alla "firma/sottoscrizione" informatica occorre tenere presente che la stessa può appartenere a due distinte categorie[5].

Distinguiamo appunto: *FIRMA DIGITALE - FIRMA ELETTRONICA*

Dette differenti sorte di sottoscrizione informatica acquistano inoltre una diversa efficacia probatoria relativamente al documento del quale rappresentano la sottoscrizione.

La firma digitale prevede la contemporanea collaborazione di tre distinti soggetti: il mittente, il destinatario e un ente appositamente abilitato (art. 1, lett. m) del D.P.R citato) a certificare lo scambio di informazioni, e a rilasciare il certificato della chiave pubblica[6]. Lo stesso ente è inoltre tenuto a custodire apposite liste ed elenchi relativi ai certificati sospesi o revocati.[7]

Passiamo ad analizzare in dettaglio, come funziona il sistema e in cosa consistono i suddetti certificati.

Per ottenere la materiale garanzia di inviare un documento informatico ottenendo la certificazione relativamente a provenienza e paternità è necessario riuscire a criptare il documento, criptazione che si ottiene mediante l'utilizzo di una "chiave"[8] detta in questo caso privata. Detta chiave privata, contenuta solitamente all'interno di un microchip, viene di norma inserita in una sorta di carta magnetica (tipo carta di credito) fornita dal gestore del servizio al soggetto che vuole utilizzare il sistema. Giunti a questo punto entra in gioco una seconda "chiave" detta invece pubblica, la cui funzione risulta quella di preservare il documento da intercettazioni esterne, questa chiave viene anche detta di de-criptazione. L'intero sistema denominato della "doppia chiave asimmetrica", risulta molto sicuro poiché utilizzando due chiavi differenti e quindi due meccanismi crittografici alternativi, pur tra loro collegati, fa si che un terzo soggetto qualsiasi, che malauguratamente venisse a trovarsi in possesso della chiave di decriptazione pubblica non sarebbe in

[5] Come vedremo esiste una sorta di terza categoria che gli esperti individuano e che corrisponde alla firma prevista con il nuovo D.P.R.

[6] Vedremo poco dopo cosa rappresenti la chiave pubblica;

[7] Si pensi a certificati che vengono persi o smarriti, chiavi/firme che quindi non forniscono più alcuna garanzia. Logico quindi che sia prevista l'esistenza di particolari elenchi che permettano di risalire a certificati non più attendibili. Lo stesso sistema è tra l'altro utilizzato per garantire l'utilizzo di carte di credito (elenchi di carte smarrite o clonate) e l'autenticità di assegni bancari (anche in questo caso esistono particolari registri informatici con la segnalazione del numero seriale di assegni rubati, smarriti o contraffatti).

[8] La "chiave elettronica" non risulta essere altro che un sistema di codifica/decodifica gestito tramite algoritmi matematici.

grado di risalire alla prima chiave, non riuscendo quindi a giungere a decifrare il testo/documento di partenza.[9]

Ovvia a questo punto la considerazione che maggiormente complesse risultano essere le chiavi/algoritmi di criptazione e decriptazione tanto più arduo risulterà, anche a un esperto di informatica risalire dalla chiave pubblica a quella privata e quindi decriptare il documento originale.[10]

Occupandoci dell'altra categoria di firma che abbiamo individuato, doveroso sottolineare come invece la firma elettronica sia stata introdotta nel nostro ordinamento solo con il D.lgs n. 10/2002, tra l'altro in attuazione di una direttiva comunitaria.

Detta firma si suddivide ulteriormente in FIRMA ELETTRONICA DEBOLE e FIRMA ELETTRONICA FORTE.

La firma debole rappresenta solamente una sequenza/riunione di dati sviluppati in forma elettronica che risultano però essere collegati tra di loro mediante procedimenti logici o mediante altri dati elettronici, collegamenti che permettono di individuare detto insieme di dati come mezzo di autenticazione informatica.

Sul versante opposto, troviamo la figura della firma elettronica avanzata. La definizione della stessa appare maggiormente difficoltosa, non trovando alcuna precisazione caratterizzante all'interno della legislazione in materia. La stessa secondo vari giuristi può essere individuata attraverso una serie di elementi costitutivi che la individuano.

La firma elettronica avanzata deve essere:

1) connessa in modo certo con il firmatario,[11]

2) idonea ad individuare quest'ultimo in modo univoco,[12]

[9] Da sottolineare che in precedenza veniva utilizzato il sistema della doppia chiave simmetrica. Detto sistema forniva garanzie minori per il semplice fatto che la chiave/algoritmo di criptazione e quella di decriptazione erano semplicemente identiche e quindi un terzo soggetto che venisse in possesso dell'una o dell'altra si trovava per forza di cose in possesso anche dell'altra chiave, rendendogli con ciò molto più facile risalire al documento originale.

[10] Da un punto di vista prettamente informatico le chiavi oggi utilizzate sono costituite da algoritmi a 1024 bits, cioè 1024 impulsi elettrici, anche se già si arriva ad algoritmi a 2048 bits, utilizzati di norma per documenti che necessitano di maggior sicurezza durante la trasmissione.

[11] Detta connessione tra firma e firmatario deve risultare materialmente riscontrabile e non deve essere solo supposta. Per connessione si intende nello specifico la possibilità di ricollegare appunto la sottoscrizione con colui che materialmente la produce.

[12] Il firmatario deve essere individuabile in modo univoco, quindi anche se esistesse la minima possibilità che la firma appartenga a più di un soggetto non risultano più riscontrabili i presupposti per parlare di firma elettronica forte.

3) deve venire creata su mezzi o supporti tecnici dei quali il firmatario abbia l'esclusivo controllo,[13]
4) deve essere collegata e connessa in modo inequivocabile agli input cui si riferisce in modo che venga evidenziato ogni, anche minimo, tentativo di manomissione o effrazione del documento stesso.[14]

Dopo aver sinteticamente parlato e descritto la consistenza materiale e tecnica circa la differenza di dette forme di firma, occorre ora arrivare al nocciolo della questione e analizzarne l'efficacia probatoria.

Per quanto concerne la firma digitale dobbiamo necessariamente fare riferimento all'art. 10 del D.P.R 445/2000[15] dove al terzo comma si specifica che l'atto sottoscritto con tale tipo di firma acquista la stessa efficacia di una scrittura privata,[16] e quindi costituisce prova piena fino a querela di falso della provenienza delle dichiarazioni da parte di chi l'ha sottoscritto. Resta comunque da sottolineare che risulta comunque necessario il riconoscimento della sottoscrizione.

Per ciò che concerne la procedura di verifica dell'eventuale disconoscimento della sottoscrizione, detta verifica risulta alquanto agevole, basta infatti la verifica e comparazione delle due chiavi, pubblica e privata, alle quali si faceva riferimento precedentemente, indipendentemente che ci si trovi in presenza di un meccanismo a doppia chiave simmetrica o asimme-

[13] Se il firmatario non fosse l'unico ad avere accesso e ad avere il controllo in esclusiva dei supporti tecnici sui quali viene creato il documento con la relativa autenticazione, nulla risulterebbe la garanzia di paternità visto che nessuna certezza sarebbe riscontrabile per ciò che concerne l'individuazione dell'autore.

[14] Un documento a paternità certa e certificata, ma non esente dalla possibilità di ingressi esterni non risulta comunque in grado di offrire la benché minima garanzia.

[15] **Articolo.10**
Forma ed efficacia del documento informatico
1. Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 e per le pubbliche amministrazioni, anche di quelle di cui all'articolo 9, comma 4, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile.
2. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro delle finanze.
3. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.
4. Il documento informatico redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

[16] Cfr. art. 2702 c.c.

trica. La corrispondenza e ricollegabilità delle due chiavi infatti sancisce inequivocabilmente la provenienza/paternità della firma digitale con gli effetti che dalla legge ne conseguono.

Per ciò che concerne invece l'efficacia probatoria della firma elettronica diverse le osservazioni che si possono apportare.

Procedendo nell'analisi del decreto legislativo n. 10 del 2002, che ha tra l'altro innovato diversi articoli del D.P.R n. 445/2000 precedentemente citato, all'articolo 6 si stabilisce e determina che il documento informatico, sottoscritto con firma elettronica, quello che abbiamo definito come "debole" soddisfa pienamente i requisiti legali richiesti a un documento avente forma scritta e quindi così come previsto dall'ordinamento italiano la sua efficacia probatoria risulterà sottoposta alla libera interpretazione da parte dell'organo giudicante[17].

Relativamente alla firma elettronica denominata "forte" basta invece sottolineare come la relativa efficacia legale venga semplicemente riportata a quella del documento sottoscritto con firma digitale.

Proseguendo nella analisi con il D.P.R n.137/2003 viene introdotta una nuova categoria di firma, frutto dell'avanzamento di tecnologia e legislazione: parliamo della firma elettronica qualificata. La stessa si riscontra appunto in presenza dei requisiti che abbiamo individuato relativamente alla firma elettronica "avanzata" e deve inoltre essere fornita di un certificato di qualità e garanzia creato mediante appositi meccanismi di sicurezza.

La firma elettronica "qualificata" per quanto concerne l'efficacia probatoria dovrebbe a questo punto rientrare tra i mezzi di prova liberamente valutati dal giudice. L'utilizzo del condizionale risulta d'obbligo ritenuto che nessuna indicazione in merito è riscontrabile all'interno del D.P.R.

Siamo a questo punto giunti ad avere delineato un sommario quadro del panorama legislativo italiano in merito alla firma digitale/elettronica e al valore della e-mail. Certamente ci troviamo in presenza di un primo semplice passo operato dal legislatore in materia, comunque una "nuova era" risulta aperta, legislazione e tecnologia risultano meno lontane, e anche se nuovi interrogativi sorgeranno in futuro, resta comunque il fatto che l'ordinamento italiano ha, tra i primi, dato il via a un percorso di regolamentazione, fornendo le prime risposte.

[17] Ovviamente la valutazione necessita di essere basata su elementi oggettivi.

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 11 febbraio 2005, n.68

Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

(Gazzetta Ufficiale n. 97 del 28-4-2005)

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87 della Costituzione;

Visto l'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;

Visto l'articolo 27, commi 8, lettera e), e 9, della legge 16 gennaio 2003, n. 3;

Visto l'articolo 17, comma 2, della legge 23 agosto 1988, n. 400;

Visto l'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 25 marzo 2004;

Espletata la procedura di informazione di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con legge 21 giugno 1986, n. 317, cosi' come modificata dal decreto legislativo 23 novembre 2000, n. 427;

Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 20 maggio 2004;

Vista la nota del 29 marzo 2004, con la quale è stato richiesto il parere del Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 14 giugno 2004;

Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 28 gennaio 2005;

Sulla proposta del Ministro per la funzione pubblica e del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze;

Emana il seguente regolamento:

Articolo 1 - Oggetto e definizioni

1. Il presente regolamento stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.
2. Ai fini del presente regolamento si intende per:
   a) busta di trasporto, il documento informatico che contiene il messaggio di posta elettronica certificata;
   b) Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: "CNIPA", l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
   c) dati di certificazione, i dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata;
   d) dominio di posta elettronica certificata, l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete;
   e) log dei messaggi, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore;
   f) messaggio di posta elettronica certificata, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
   g) posta elettronica certificata, ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;
   h) posta elettronica, un sistema elettronico di trasmissione di documenti informatici;
   i) riferimento temporale, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
   l) utente di posta elettronica certificata, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonchè eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;
   m) virus informatico, un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Articolo 2 - Soggetti del servizio di posta elettronica certificata

1. Sono soggetti del servizio di posta elettronica certificata:
   a) il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
   b) il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
   c) il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Articolo 3 - Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:
   "1. 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.".

Articolo 4 - Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge.
2. Per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi e le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e puo' essere revocata nella stessa forma.
3. La volontà espressa ai sensi del comma 2 non puo' comunque dedursi dalla mera indicazione dell'indirizzo di posta certificata nella corrispondenza o in altre comunicazioni o pubblicazioni del soggetto.
4. Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e puo' essere revocata nella stessa forma.
5. Le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione

della disponibilità, nonchè le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17.

6. La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6.
7. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono di uno dei gestori di cui agli articoli 14 e 15.

Articolo 5 - Modalità della trasmissione e interoperabilità

1. Il messaggio di posta elettronica certificata inviato dal mittente al proprio gestore di posta elettronica certificata viene da quest'ultimo trasmesso al destinatario direttamente o trasferito al gestore di posta elettronica certificata di cui si avvale il destinatario stesso; quest'ultimo gestore provvede alla consegna nella casella di posta elettronica certificata del destinatario. 2. Nel caso in cui la trasmissione del messaggio di posta elettronica certificata avviene tra diversi gestori, essi assicurano l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

Art. 6 - Ricevuta di accettazione e di avvenuta consegna

1. Il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata.
2. Il gestore di posta elettronica certificata utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna.
3. La ricevuta di avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.
4. La ricevuta di avvenuta consegna puo' contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.
5. La ricevuta di avvenuta consegna è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.

6. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di una busta di trasporto valida secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
7. Nel caso in cui il mittente non abbia piu' la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Articolo 7 - Ricevuta di presa in carico

1. Quando la trasmissione del messaggio di posta elettronica certificata avviene tramite piu' gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio.

Articolo 8 - Avviso di mancata consegna

1. Quando il messaggio di posta elettronica certificata non risulta consegnabile il gestore comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna tramite un avviso secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 9 - Firma elettronica delle ricevute e della busta di trasporto

1. Le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute stesse secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
2. La busta di trasporto è sottoscritta con una firma elettronica di cui al comma 1 che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 10 - Riferimento temporale

1. Il riferimento temporale e la marca temporale sono formati in conformità a quanto previsto dalle regole tecniche di cui all'articolo 17.
2. I gestori di posta elettronica certificata appongono un riferimento temporale su ciascun messaggio e quotidianamente una marca temporale sui log dei messaggi.

Articolo 11 - Sicurezza della trasmissione

1. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto.
2. Durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi.
3. Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.
4. I gestori di posta elettronica certificata prevedono, comunque, l'esistenza di servizi di emergenza che in ogni caso assicurano il completamento della trasmissione ed il rilascio delle ricevute.

Articolo 12 - Virus informatici

1. Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.
2. Qualora il gestore del destinatario riceva messaggi con virus informatici è tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente, affinchè comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

Art. 13 - Livelli minimi di servizio

1. I gestori di posta elettronica certificata sono tenuti ad assicurare il livello minimo di servizio previsto dalle regole tecniche di cui all'articolo 17.

Art. 14 - Elenco dei gestori di posta elettronica certificata

1. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.
2. Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.

3. I richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro.
4. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione devono, inoltre, possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.
5. Non possono rivestire la carica di rappresentante legale, di componente del consiglio di amministrazione, di componente del collegio sindacale, o di soggetto comunque preposto all'amministrazione del gestore privato coloro i quali sono stati sottoposti a misure di prevenzione, disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, e della legge 31 maggio 1965, n. 575, e successive modificazioni, ovvero sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione, alla reclusione non inferiore ad un anno per delitti contro la pubblica amministrazione, in danno di sistemi informatici o telematici, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, ovvero per un delitto in materia tributaria.
6. Il richiedente deve inoltre:
   a) dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;
   b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;
   c) rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 17;
   d) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
   e) utilizzare per la firma elettronica, di cui all'articolo 9, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;
   f) adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;
   g) prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;

h) fornire, entro i dodici mesi successivi all'iscrizione nell'elenco dei gestori di posta elettronica certificata, dichiarazione di conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti, relativa al processo di erogazione di posta elettronica certificata;

i) fornire copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.

7. Trascorsi novanta giorni dalla presentazione, la domanda si considera accolta qualora il CNIPA non abbia comunicato all'interessato il provvedimento di diniego.
8. Il termine di cui al comma 7 puo' essere interrotto una sola volta esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
9. Il procedimento di iscrizione nell'elenco dei gestori di posta elettronica certificata di cui al presente articolo puo' essere sospeso nei confronti dei soggetti per i quali risultano pendenti procedimenti penali per delitti in danno di sistemi informatici o telematici.
10. I soggetti di cui al comma 1 forniscono i dati, previsti dalle regole tecniche di cui all'articolo 17, necessari per l'iscrizione nell'elenco dei gestori.
11. Ogni variazione organizzativa o tecnica concernente il gestore ed il servizio di posta elettronica certificata è comunicata al CNIPA entro il quindicesimo giorno.
12. Il venire meno di uno o piu' requisiti tra quelli indicati al presente articolo è causa di cancellazione dall'elenco.
13. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1.

Articolo 15 - Gestori di posta elettronica certificata stabiliti nei Paesi dell'Unione europea

1. Puo' esercitare il servizio di posta elettronica certificata il gestore del servizio stabilito in altri Stati membri dell'Unione europea che soddisfi, conformemente alla legislazione dello Stato membro di stabilimento, formalità e requisiti equivalenti ai contenuti del presente decreto e operi nel rispetto delle regole tecniche di cui all'articolo 17. è fatta salva in particolare, la possibilità di avvalersi di gestori stabiliti in altri Stati membri

dell'Unione europea che rivestono una forma giuridica equipollente a quella prevista dall'articolo 14, comma 3.
2. Per i gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea il CNIPA verifica l'equivalenza ai requisiti ed alle formalità di cui al presente decreto e alle regole tecniche di cui all'articolo 17.

Articolo 16 - Disposizioni per le pubbliche amministrazioni

1. Le pubbliche amministrazioni possono svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata, oppure avvalersi dei servizi offerti da altri gestori pubblici o privati, rispettando le regole tecniche e di sicurezza previste dal presente regolamento.
2. L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata. 3. Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.
4. Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative.

Articolo 17 - Regole tecniche

1. Il Ministro per l'innovazione e le tecnologie definisce, ai sensi dell'articolo 8, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sentito il Ministro per la funzione pubblica, le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi è acquisito il concerto del Ministro delle comunicazioni.

Articolo 18 - Disposizioni finali

1. Le modifiche di cui all'articolo 3 apportate all'articolo 14, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, (Testo A) si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. è fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.
Dato a Roma, addi' 11 febbraio 2005

BIBLIOGRAFIA

F.Luiso, *Diritto Processuale Civile*, Milano, Giuffrè Editore, 2000,
L.Turini, "Il valore probatorio del messaggio di posta elettronica", in *Ventiquattrore Avvocato*, anno 1, n°1, Milano, Ed. Il Sole 24 ore, 2004
D.P.R 11 febbraio 2005, n.68
http://www.altalex.com/index.php?idstr=39&idnot=7964
http://www.cittadinolex.kataweb.it/article_view.jsp?idArt=28362&idCat=272