LA TRASMISSIONE
DEL DOCUMENTO INFORMATICO
MEDIANTE POSTA ELETTRONICA

Versione 1.0

N.B.: ogni altra precedente versione di questo scritto eventualmente pubblicata sotto ogni forma deve ritenersi solo una bozza e non può considerarsi in alcun modo a me attribuibile a me.

Indice

NOTE LEGALI

PREFAZIONE

- Sezione non modificabile –

A proposito dei limiti di utilizzo del mio scritto, preciso quanto segue.

Quel poco che so di informatica lo devo – oltre che alla mia innata curiosità - all'aiuto disinteressato di un mio fraterno amico (Antonio Valiante) e alla lettura di tanto materiale reperito in Rete.

L'HTML, per esempio, l'ho appreso non solo smanettando, ma anche frequentando il forum di www.html.it. Ho imparato a scrivere pagine ASP grazie ai tutorial di Darty, pubblicate sul suo sito www.amicopc.com, e alle sue dritte.

In questi anni, insomma, ho "incontrato" in Rete tante persone generose, le quali non mi hanno lesinato preziosi suggerimenti. E ciò, pur ignorando che io – svolgendo la professione di avvocato - non ero un loro potenziale concorrente.

Avendo, quindi, ricevuto tanto da tanti, sento l'obbligo morale di dare anch'io un modesto contributo.

Perciò, ho deciso di pubblicare questo mio lavoro secondo i termini della *GNU Free Documentation License*, versione 1.1 o qualsiasi versione successiva pubblicata dalla *Free Software Foundation*.

Peraltro, anche altre considerazioni mi hanno indotto a tale forma di pubblicazione.

I temi trattati in questo scritto sono solo un primo e parziale tentativo – portato a termine in un momento in cui, per quanto mi risulta, non esiste ancora giurisprudenza - di inquadrare i tanti problemi giuridici connessi alla trasmissione del documento informatico.

Ritengo, quindi, che la "filosofia dell'*open source*" sia quella più efficace per ampliare, approfondire ed aggiornare lo studio degli argomenti trattati.

Consapevole sia della difficoltà di perseguire tale fine - mantenendo al tempo stesso una pur necessaria organicità dell'opera - e sia dei miei limiti, ho chiesto ed ottenuto la promessa di collaborazione dell'ingegnere **LUCA MARLETTA**[1] di Como.

Pertanto, è consentita la riproduzione, la distribuzione e/o la modifica di questo documento.

Inoltre, eventuali contributi saranno molto apprezzati!

[1] L'ing. Luca Marletta è consulente di strategia e tecnologia Internet, il suo sito è al seguente URL: http://www.behavior.it/be/index.php

Chiunque potrà fornire un aiuto a questo progetto di studio in molti modi: chi ha molto tempo a disposizione, potrà scrivere un capitolo intero. Ma sarà ben accetto ogni suggerimento su come migliorare il contenuto.

E non avendo letto invano anche qualche pagina di Platone, apprezzerò ancor più le confutazioni[2]!

Ringrazierò, poi, anche per le segnalazioni dei refusi.

Leonardo Perone,
attuale indirizzo di posta elettronica: *leoper@iol.it*

---

[2] Così Platone nel dialogo *Il Sofista, 230-d*:

[....]

Straniero: *Per tutti questi motivi, Teeteto, noi dobbiamo asserire che la confutazione è la massima e la più efficace delle purificazioni e dobbiamo anche ritenere che chi non è stato confutato, fosse pure il Gran Re, non essendo purificato nelle cose più importanti, è privo di educazione e brutto proprio in ciò in cui, a chi intende essere realmente felice, converrebbe essere più puro e più bello"*

[....]

INTRODUZIONE

Nelle pagine seguenti mi propongo di esporre alcune considerazioni sulla trasmissione del documento informatico mediante posta elettronica.

In particolare, tralasciando ogni riferimento al tipo di documento trasmesso, tratterò i seguenti problemi:

- il coordinamento dell'art. 14 del T.U. 445/2000 con le norme contenute nel codice civile a proposito delle dichiarazioni recettizie;
- la prova della trasmissione del documento informatico mediante il sistema la posta elettronica; e, ciò sia nel caso in cui essa avvenga con quella ordinaria che con quella cd. certificata.

Per tentare di dare ad essi una soddisfacente risposta, affronterò preliminarmente gli aspetti tecnici di tale sistema, la cui esatta comprensione mi sembra indispensabile per una corretta interpretazione delle norme, che lo regolano.

LA POSTA ELETTRONICA CONSIDERATA DAL PUNTO DI VISTA DELL'INFORMATICO

L'operazione di inviare e leggere un messaggio di posta elettronica, che i moderni programmi di posta hanno ridotto a pochi azzeccati click, si basa in realtà su un meccanismo alquanto complesso, la cui comprensione è indispensabile per lo studio dei problemi che ci occupano.

Ciò mi induce, preliminarmente, a spiegarne nei limiti del possibile e dell'indispensabile il funzionamento, prendendo in considerazione l'ipotesi più comune in cui l'invio e la ricezione dei messaggi avviene tra soggetti collegati a Internet tramite un ISP, i quali hanno ottenuto un accesso (account) presso un elaboratore dell'ISP, che costituisce anche il recapito per la posta elettronica, con la possibilità di utilizzare un servente SMTP per l'invio della posta elettronica[3].

Il sistema di trasporto della posta elettronica

Nell'ipotesi più comune – l'unico preso in esame - esso si basa sulla cooperazione di due tipi di sottosistemi: Mail User Agent *(MUA)* e Mail Transport Agent *(MTA)*

1.1.1 Il MUA

Il MUA – o "agente utente" – costituisce l'interfaccia dell'utente con il client. Esso è un programma di gestione di posta (Outlook, Eudora, …), che consente all'utente almeno di leggere e scrivere messaggi ed è spesso l'unica parte del sistema di posta elettronica che l'utente medio percepisce allorché invia e riceve i messaggi e svolge i suoi compiti (composizione, trasferimento, notifica, visualizzazione ed eliminazione dei messaggi) grazie alle seguenti caratteristiche:

- ✓ Possiede un'interfaccia che consente all'utente di comporre, inviare, ricevere e leggere i

[3] quindi, per esempio, non esaminerò le seguenti ipotesi:

un sistema composto da un elaboratore isolato con terminali più o meno decentrati; in tale situazione, vi sarà alcun bisogno di fare viaggiare messaggi attraverso una rete, essendo sufficiente che questi vengano semplicemente messi a disposizione dell'utente destinatario (in un file contenuto nella sua directory personale, o in una directory pubblica, in cui il file in questione possa essere accessibile solo a quell'utente particolare). In tal caso, sarà un MDA, ovvero Mail delivery agent, ad avere il compito di attuare questo sistema;

chi - avendo ottenuto un numero IP statico e quindi un nome di dominio per il proprio nodo - scelga di ricevere direttamente lì la posta. In tal caso, si dovrà attivare un server SMTP locale, che provveda direttamente alla consegna dei messaggi ricevuti.

messaggi.

- ✓ Conosce il protocollo SMTP per spedire i messaggi, ovvero colloquiare con un server SMTP (MTA), che ne cura la trasmissione;
- ✓ Conosce la sintassi di composizione dei messaggi (RFC822 e MIME).
- ✓ Conosce il protocollo POP3 e IMAP4, per ricevere i messaggi da un MTA;

1.1.2 L'MTA

L'MTA – o "agente di trasferimento" – ha sostanzialmente una funzione di "ponte" tra due MUA. Esso costituisce l'interfaccia con la rete e si occupa di ricevere e trasmettere i messaggi.

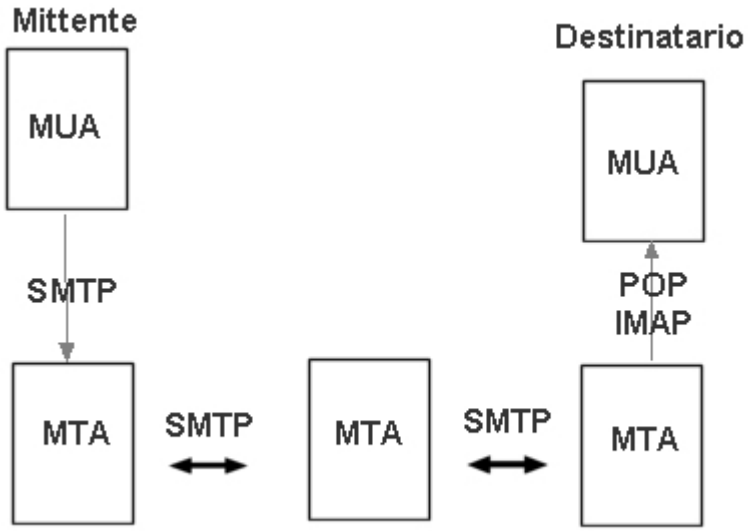
In pratica, analogamente a quanto avviene per la posta ordinaria, la spedizione di un e-mail si basa su di un meccanismo chiamato relay (staffetta): il messaggio viene dato in carico dal MUA al più vicino server di posta SMTP (che è appunto un MTA), il quale provvede – direttamente, ovvero servendosi di un altro server SMTP più vicino a quello di destinazione (anch'esso MTA) - a consegnarlo al server che mantiene la casella di posta del destinatario (altro MTA).

Il trasferimento verso la destinazione finale di un messaggio può, quindi, interessare diversi MTA, i quali utilizzano per comunicare il protocollo SMTP.

L'MTA può essere:

- ✓ un server SMTP che gestisce la spedizione e la ricezione dei messaggi verso e da altri server SMTP
- ✓ un server POP3 che gestisce la spedizione dei messaggi al client di posta;
- ✓ un server IMAP4 che permette la gestione dei messaggi sul server dal client di posta.

Il sistema di posta elettronica può essere dunque così rappresentato:



L'invio e il percorso dei messaggi – Il protocollo SMTP

Come si è sopra accennato, gli MTA comunicano tra loro utilizzando prevalentemente il protocollo SMTP[4] *(Simple Mail Transfer Protocol*), definito nel 1982 dal gruppo IETF *(Internet Enginnering Tas Force)* e specificato dalle RFC *(Request for Comment)* 821 e 822[5]. Ma anche il MUA

[4] Precisiamo, per completezza, che esistono due standard di posta elettronica: X.400 e SMTP. Ci limiteremo a trattare il secondo perché è il più diffuso e anche il legislatore ha preso atto di tale realtà. Cfr. le seguenti norme:

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 - Art. 15 - Modalità di trasmissione e registrazione dei documenti informatici, comma 1° (*1. Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.)*

Autorità per l'informatica nella pubblica amministrazione - Circolare 7 maggio 2001, n. AIPA/CR/28 , 6° comma (Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni distribuite sul territorio è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete. Ai sensi del D.P.C.M. 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi. [….])

Autorità per l'informatica nella pubblica amministrazione - Circolare 7 maggio 2001, n. AIPA/CR/28 - Allegato A- Art. 4. Formato di codifica, 1° comma *(Come stabilito dall'articolo 15, comma 1, del D.P.C.M. 31 ottobre 2000, i messaggi scambiati tra le AOO devono essere compatibili con i sistemi di posta elettronica che adottano lo standard SMTP, descritto nelle specifiche pubbliche RFC 821 e RFC 822.)*

Autorità per l'informatica nella pubblica amministrazione - Circolare 7 maggio 2001, n. AIPA/CR/28 - Allegato A- Art. 6. Messaggi di ritorno, 3° comma *(I messaggi di ritorno, inviati da una AOO ricevente a scopo informativo, sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME. […])*

[5] Per completezza, si precisa che il protocollo in esame è descritto nella RFC 821, ma lavora in stretta collaborazione con

La nota continua alla pagina successiva

impiega tale protocollo per comunicare con un MTA nella fase d'invio dei messaggi di posta. Viceversa, i MUA li ricevono utilizzando i seguenti protocolli: IMAP *(Internet Message Access Protocol)* o POP *(Post Office Protocol),* di cui diremo più avanti.

Soffermiamoci per il momento sul protocollo SMTP, che – come si è detto - è quello utilizzato per l'invio di un messaggio sia da un MUA ad un MTA che e da un MTA all'altro.

SMTP utilizza il protocollo di trasporto TCP, ed in particolare un SMTP server rimane costantemente in ascolto sulla porta 25. Il server SMTP si occupa poi di trasferire i messaggi nelle caselle di posta (mailbox) dei destinatari, oppure qualora non fosse il diretto responsabile di queste, inoltrarli (ecco il relay!) al server che provvederà a tale compito.

Una sessione SMTP attraversa, quindi, almeno le sei seguenti fasi:

1. il client, utilizzando una porta scelta a caso maggiore di 1024, contatta mediante protocollo SMTP il server (che utilizza la porta TCP 25), il quale, se è in ascolto e accetta la connessione, risponde con un messaggio che dichiara la propria disponibilità a ricevere (220, ovvero *Ready*);

2. a quel punto, il client chiede di stabilire la sessione SMTP e si "presenta" inviando il comando HELO seguito dal proprio FQDN *(Fully Qualified Domani Name)*. Se il server accetta il "dialogo", lo dichiara con un messaggio (250, <Ok>);

3. il client comunica, quindi, l'indirizzo di posta del mittente tramite il comando MAIL FROM: <*indirizzo mittente*> e riceve dal server un altro messaggio che lo invita a proseguire (250, <Ok>)*;*

---

altri standard come quelli definiti dalla RFC 822 (che descrive la sintassi degli headers della mail), dalla RFC 1049 (che definisce le strutture dati per interpretare correttamente il contenuto delle mail) e dalla RFC 974 che si occupa del routing delle mail tramite DNS.

Lo standard definito dalla RFC 821, aveva diversi limiti riguardanti per esempio la dimensioni dei messaggi oppure la trasmissione di mail non in inglese o diverse dal semplice plain text. Per ovviare a questa restrizione è stato necessario estendere il protocollo tramite la RFC 1425 riguardante le SMTP Service Extensions.

Così, l'autore dello scritto pubblicato sotto GNU FDL al seguente URL:
http://openskills.info/livebooks/statics/guida_ai_protocolli_internet/il_protocollo_smtp.htm

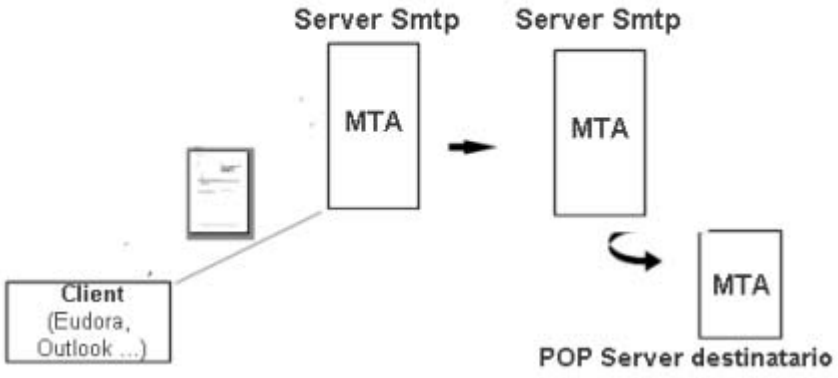
4. successivamente il client indica al server i destinatari del messaggio tramite il comando RCPT TO: <*indirizzo destinatario*> ed il server risponde per ogni destinatario accettato con il solito tranquillizzante messaggio positivo (250,<Ok>);

5. ultimate queste operazioni preliminari, il client comunica al server, mediante il comando DATA, l'intenzione di trasmettere il corpo del messaggio. Il server risponde con un codice 354 e indica come marcare il termine del messaggio. I campi come Date, Subject, To, Cc, From vanno inseriti tra i dati della mail;

6. completato il messaggio da scrivere, il server memorizza la mail. A questo punto è possibile, comunicare al server l'intenzione di trasmettere un nuovo messaggio (grazie al già visto comando MAIL FROM) oppure di terminare la sessione SMTP, servendosi del comando QUIT, al che il server invia i messaggi e risponde con un codice 221 (Closing) e comunicando così che la connessione TCP è terminata.[6]

L'esempio di log riportato alla nota 10, consentirà di comprendere meglio le fasi sopra descritte.

La prima parte del normale cammino di un messaggio di posta può, quindi, essere rappresentata dal seguente grafico.



[6] Cfr. Brian Komar, TCP/IP Guida completa, 2001, Apogeo, pag. 295

Vi è da evidenziare che, a differenza dell'IMAP e del POP, la forma più elementare di SMTP non richiede alcuna autenticazione. Ciò significa che i server SMTP possono permettere a qualunque utente di Internet di utilizzare il sistema per inviare o trasmettere la posta a un numero imprecisato di destinatari. Il che - oltre a rendere possibile il fenomeno dello spam – non consente un'indubbia individuazione del reale mittente. Deve anche dirsi, però, che le applicazioni SMTP moderne minimizzano ormai questo comportamento, riducendo la possibilità di ritrasmissione e consentendo l'invio di posta solo agli host conosciuti[7].

[7] La RFC-821 – come si è detto nella nota precedente – definisce il comportamento di base dell'SMTP. Tuttavia, negli anni, molte estensioni SMTP possibili grazie a RFC-1869 hanno aggiunto ulteriori funzioni a questo protocollo, rendendo disponibili nuovi comandi. Inizializzando una conversazione con un server SMTP con il comando EHLO piuttosto che HELO, il server per la connessione identifica se stesso come un server che supporta le estensioni SMTP. Il server ricevente risponde con una riga 250 contenente le diverse estensioni SMTP supportate. Il server di connessione può quindi usare le estensioni supportate per la comunicazione.

Un'importante estensione riguarda l'inserimento dell'Autenticazione SMTP mediante il comando AUTH come evidenziato in RFC-2554. Un'altra estensione molto diffusa viene descritta nel dettaglio in RFC-2034, la quale tratta l'utilizzo di codici d'errore standardizzati e separati dal punto, necessari tra applicazioni SMTP. La lettura dei vari RFC riguardanti l'SMTP fornisce informazioni di base sui percorsi Internet dei messaggi di posta elettronica. È inoltre possibile connettersi a un server SMTP via telnet specificando la porta 25, per esempio telnet localhost 25.

La verifica dei messaggi - I protocolli IMAP e POP

Per accedere ai messaggi di posta presenti su un MTA, un MUA utilizza uno dei seguenti protocolli: IMAP e POP. Spendiamo qualche parola anche in merito ad essi.

1.1.3 Protocollo IMAP

L'Internet Message Access Protocol (IMAP) è uno dei protocolli usati dalle applicazioni client di e-mail per accedere ai messaggi archiviati in remoto. Esso è caratterizzato da una maggiore ricchezza di funzioni e complessità, in quanto consente all'utente di modificare la propria casella di posta come se fosse sulla propria macchina.

La caratteristica più interessante per i fini che ci occupano consiste in ciò. Utilizzando il protocollo IMAP, i messaggi di posta elettronica rimangono sul server, dove l'utente può leggerli (anche solo in parte), con la libertà di decidere se cancellarli, creare, rinominare o eliminare caselle di posta per archiviare le e-mail.

Per altre informazioni, rimando alle Request for Comment (RFC) che coprono l'IMAP, le quali contengono diversi dettagli e specifiche sul funzionamento del protocollo. In particolare, la RFC-1730 definisce le modalità d'utilizzo di IMAP nella versione 4, mentre la RFC-2060 tratta l'implementazione IMAP corrente usata da numerosi server IMAP, la versione IMAP4rev1.

Altre utili informazioni sulle caratteristiche di tale protocollo sono reperibili al seguente URL: http://www.europe.redhat.com/documentation/rhl8.0/rhl-rg-it-8.0/ch-email.php3.

1.1.4 Protocollo POP

Il Post Office Protocol (POP)[8] consente ai MUA di connettersi agli MTA e di "scaricare" i messaggi di posta elettronica dal server remoto al computer locale. A tale proposito deve rilevarsi che la maggior parte dei client POP di e-mail è configurata in modo da eliminare automaticamente il messaggio sul mail server allorché esso è trasferito con successo sul sistema del destinatario.

Ma vediamo come le varie fasi della "ricezione" della posta con tale protocollo.

Pur esistendo tre versioni diverse di tale protocollo, l'unica di fatto utilizzata è la versione 3(POP3).

1. fase di instaurazione della connessione. Per connettersi a un server POP, il client di e-mail apre una connessione TCP sulla porta 110 del server;

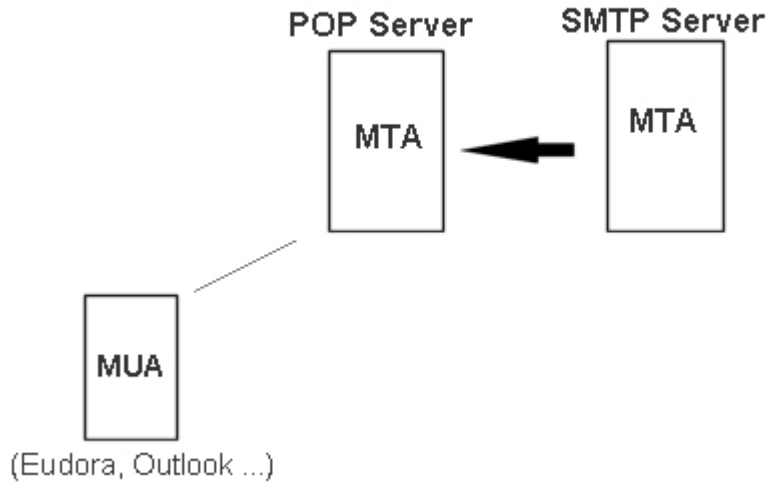
2. fase di autenticazione. Una volta effettuata la connessione, il server POP si presenta al client POP e i due cominciano a scambiarsi comandi e risposte specificati nel protocollo. In particolare in tale fase il MUA invia al server POP "nome utente" e "password" dell'utente. Una volta che è stata verificata l'esistenza di una mailbox corrispondente ad esso e la corrispondenza della password, si passa alla fase successiva;

3. fase di transazione. Attraverso comandi quali LIST, RETR e DELE - rispettivamente per elencare, scaricare ed eliminare i messaggi dal server – il MUA recupera i messaggi. Nel caso in cui esso sia stato settato per la loro eliminazione, essi sono rimossi dal server. Ma ciò solo allorché il client POP invia il comando QUIT per terminare la sessione;

4. fase di aggiornamento. Il server POP esegue l'eventuale comando per la cancellazione dei messaggi ed elimina qualsiasi risorsa residua dalla sessione.

In buona sostanza, impiegando il protocollo in esame, la lettura della posta si risolve nel "prendere" ciò che si trova sul server e nel trasportarlo sul proprio elaboratore. Ciò comporta il grosso limite di rendere impossibile ogni controllo preventivo sulla natura dei messaggi.

Il normale accesso ai messaggi di posta presenti su un MTA utilizzando il protocollo POP, può essere, quindi, rappresentata dalla seguente immagine:



Le intestazioni dei messaggi di posta

Come si è detto, l'utente medio ignora del sistema di posta elettronica tutto quello che "è al di là" del proprio MUA. Egli, però, avverte che non tutto è semplice come sembra, allorché ha sotto gli occhi le "intestazioni (o *headers*) di un messaggio.

Infatti, i messaggi di posta ricevuti – essendo fondamentalmente composti da una sorta di busta che "accompagna" la comunicazione vera e propria - mantengono traccia del loro percorso appunto nelle cd. intestazioni e da un'analisi accurata è possibile rilevare una quantità d'informazioni: non solo il mittente, la data d'invio, il destinatario, ma anche tutti i punti d'arresto della mail nel suo percorso dal primo all'ultimo MTA[9].

[9] Consideriamo il seguente esempio. Si tratta dell'intestazione di un messaggio "interpretato" dal software SamSpade, in grado di "aiutare ad interpretarla". Per una migliore comprensione, le righe di commento aggiunte da detto programma sono riportate in corsivo:

```
Return-Path: <destinatario@iol.it>
Received: from smtp3.libero.it (193.70.192.127) by
 ims4d.libero.it (7.0.019) id 3FABEAF4003181C4 for
 mittente@iol.it; Thu, 20 Nov 2003 19:08:32 +0100
This received header was added by your mailserver ims4d.libero.it received this from
smtp3.libero.it (IP addresses match)
Received: from s2bwv82gm8wja88 (151.26.83.32) by
 smtp3.libero.it (7.0.020-DD01) id 3F6F04A60132D412;
 Thu, 20 Nov 2003 19:08:31 +0100
 smtp3.libero.it received this from someone claiming
 to be s2bwv82gm8wja88
```

La nota continua alla pagina successiva

L'esame delle intestazioni di un messaggio è, quindi, molto utile ai fini che ci occupano, ma non esaustivo, in quanto deve tenersi conto dei seguenti problemi:

- le indicazioni contenute nelle testate dei messaggi sono scarsamente attendibili, essendo alquanto facile "ingannare" un'MTA[10];
- essendo costruite dall'azione dei vari MTA implicati nelle operazioni di trasporto del messaggio, esse sono a disposizione solo del destinatario del messaggio, il quale può alterarle alquanto facilmente.
- nessuna notizia sulla sorte del messaggio inviato è "nelle mani" del suo mittente[11].

```
This doesn't match the IP address in the headers, so this may be a relay point. If so all
headers below are probably forged. It really came from ppp-32-83.26 151.libero.it
Message-ID: <002001c3af91$3611a2b0$20531a97@s2bwv82gm8wja88>
From: "Avv. cicerone" <destinatario@iol.it>
To: <Undisclosed-Recipient:;>
Subject: Fw: prova
Date: Thu, 20 Nov 2003 19:07:48 +0100
MIME-Version: 1.0
Content-Type:
 multipart/mixed; boundary="----=_NextPart_000_001C_01C3AF99.96516680"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
```

[10] La debolezza del protocollo SMTP dal punto di vista della sicurezza consente facilmente la contraffazione dei messaggi di posta o di far sì che essi sembrino provenire da un finto mittente. Al riguardo occorre ricordare che è possibile connettersi ad un server di posta SMTP ed eseguire mediante TELNET i comandi che utilizzerebbe l'MTA. Un esame più attento delle intestazioni del messaggio consente, però, di rilevare almeno le più grossolane contraffazioni.

[11] Alcuni MUA elaborano dei log di trasmissione de messaggio (di seguito ne riportiamo un esempio), ma naturalmente essi possono documentare solo l'invio del messaggio al server di posta del mittente (o anche a quello del destinatario, se il MUA ha questa funzionalità). Non altro.

25/11/2003 23.17.08 Connecting to Host mail.iol.it [Connection: ISP]

25/11/2003 23.17.08 < 220 smtp1.libero.it ESMTP Service (7.0.020-DD01) ready

25/11/2003 23.17.08 > HELO nomedominio.it

25/11/2003 23.17.08 < 250 smtp1.libero.it

25/11/2003 23.17.09 > MAIL FROM:<info@nomedominio.it>

25/11/2003 23.17.09 < 250 MAIL FROM:<info@nomedominio.it> OK

25/11/2003 23.17.09 > RCPT TO:<destinatario@nomedominiodestinatario.de>

25/11/2003 23.17.09 < 250 RCPT TO:<destinatario@nomedominiodestinatario.de> OK

La nota continua alla pagina successiva

Naturalmente le fasi di trasmissione del messaggio sopra descritte sono documentate dai files di log creati dei vari MTA in essa coinvolti; log che, se esaminati congiuntamente, consentiranno di ricostruire con un ragionevole grado di completezza ed attendibilità il percorso seguito dal singolo messaggio di posta.

25/11/2003 23.17.09 > DATA

25/11/2003 23.17.09 < 354 Start mail input; end with <CRLF>.<CRLF>

25/11/2003 23.17.11 > .

25/11/2003 23.17.12 < 250 <3F6F0E48014AD76F> Mail accepted

25/11/2003 23.17.12 > QUIT

25/11/2003 23.17.12 < 221 smtp1.libero.it QUIT

LA POSTA ELETTRONICA CONSIDERATA DAL PUNTO DI VISTA DEL GIURISTA

Ritenendo di aver assolto il compito di illustrare gli aspetti tecnici salienti del meccanismo di trasmissione della posta elettronica, passo a considerare i problemi giuridici oggetto di questo studio.

Il Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 prevede espressamente la possibilità di trasmettere per via telematica un documento informatico e ne regola gli effetti all'art. 14[12].

Tale norma[13] – apparentemente di facile interpretazione - pone a ben vedere non pochi problemi di coordinamento con quelle che regolano altri istituti; problemi, che - per quanto mi risulta – oltre a non essere stati finora portati all'attenzione di alcun giudice, sono stati solo incidentalmente affrontati in dottrina.

Ciò detto, mi accingo a spiegare i dubbi, che suscita in me la lettura di questa disposizione e a tentare di venirne a capo tenendo conto della giurisprudenza e degli studi in materia dei vari istituti, da un lato, e delle caratteristiche tecniche del sistema di trasmissione della posta elettronica, dall'altro.

Mi soffermerò, dapprima sul concetto di "indirizzo elettronico dichiarato e, poi, sui problemi relativi alla prova della trasmissione del documento informatico, esaminando sia il caso in cui essa avvenga attraverso il sistema normale sopra descritto e sia quello in cui si impiegata la cd. posta elettronica certificata.

---

[12] Articolo 14 (R) - Trasmissione del documento informatico

1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato.

2. 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 e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi.

3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

[13] Giova ricordare che essa – pure avendo natura regolamentare - dispone in materia, che è stata oggetto di delegificazione a seguito dell'entrata in vigore dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

Il concetto di indirizzo di posta dichiarato

Inizio a parlare di questo problema, ricordando brevemente che per i contratti bilaterali il nostro Codice Civile ha scelto - tra i vari sistemi possibili (dell'accettazione, della spedizione, della ricezione, della cognizione) - appunto quest'ultimo, sicché per la loro conclusione è necessario che il proponente prenda effettiva conoscenza dell'accettazione.

In generale, quindi, per l'efficacia di ogni manifestazione è necessaria l'effettiva cognizione. Il che induce parte della dottrina a ritenere più corretto definire come "cognitizie", anziché "recettizie" le manifestazioni di volontà che concorrono alla formazione dei contratti. [14]

Peraltro, l'articolo 1335 c.c.[15] pone per le dichiarazioni recettizie (o cognitizie, se si accoglie tale dottrina) un temperamento a tale sistema, sancendo una presunzione (sul piano della prova) e una limitazione sostanziale, fondata sul principio della responsabilità.

La prima (*presunzione di conoscenza*), consiste nell'inversione dell'onere della prova, in base alla quale la dichiarazione si considera conosciuta nel momento in cui giunge all'indirizzo del destinatario, sicché l'emittente dovrà provare solo di aver fatto quello che poteva per provocare in quello l'evento della conoscenza. Tocca al destinatario, dunque, provare il contrario e, cioè, che non ha conosciuto l'atto o che l'ha conosciuto in un momento diverso da quello della ricezione, con tutti gli effetti che ne conseguono. Sennonché, tale prova è addirittura irrilevante, se per sua colpa egli è stato nell'impossibilità dei avere conoscenza della dichiarazione pervenutagli. Ecco, dunque, una vera e propria limitazione al principio dell'affettiva conoscenza dell'atto, la quale è accompagnata pur essa da un'inversione dell'onere della prova: sarà, infatti, il destinatario a dover provare di non essere stato in colpa.

Orbene, in base all'art. 14 T.U. 445/2000, la trasmissione di documento elettronico al destinatario all'indirizzo di posta elettronica dichiarato rende operante la presunzione di conoscenza

---

[14] Cfr. Luigi Cariota Ferrara, *Il negozio giuridico nel diritto privato italiano*, pp. 125 e ss., Napoli, Morano editore

[15] Art. 1335 Codice Civile

La proposta, l'accettazione e la loro revoca e ogni altra dichiarazione diretta ad una determinata persona si reputano conosciute nel momento in cui giungono all'indirizzo del destinatario, se questi non prova di essere stato senza sua colpa, nell'impossibilità di averne notizia.

stabilita dalla prima parte dell'art. 1335 c.c..

Ciò detto, credo che sia lecito chiedersi non solo se "l'indirizzo elettronico" di cui parla l'art. 14 del T.U. 445/ 2000 possa essere pienamente[16] ed incondizionatamente equiparato al concetto d'"indirizzo" cui fa riferimento l'art. 1335 c.c., ma soprattutto, cosa debba intendersi per "indirizzo elettronico dichiarato".

Una soddisfacente risposta a tali quesiti può venire dall'esame della copiosa giurisprudenza formatasi sul citato art. 1335.

Le sentenze esaminate, consentono di enucleare i seguenti punti fermi dai quale partire:

- la presunzione fissata dalla norma citata è applicabile a tutte le dichiarazioni ricettizie, anche al di fuori dell'ambito negoziale[17];
- essa non e' connaturale ad alcuno specifico mezzo di trasmissione della dichiarazione diretta a persona determinata, né soggiace alle norme che regolano lo strumento di comunicazione prescelto, essendo sufficiente l'accertamento della sussistenza o no di circostanze ed elementi tali, anche se di natura presuntiva, da far ritenere l'arrivo dell'atto all'indirizzo del destinatario

---

[16] Non può tacersi, per esempio, il problema già da altri evidenziato dell'incidenza del combinato disposto degli artt. 1335 c.c. e 14 T.U. 445/2000 sul luogo della formazione dei contratti consensuali. Infatti, deve ritenersi che il contratto si perfezioni nel momento in cui il documento informatico contenente l'accettazione di una proposta contrattuale pervenga all'indirizzo di posta dichiarato del proponente, come definito dall'art. 1. lett h) del T.U. 445/2000. E, poiché la conclusione del contratto determina non solo il momento in cui sorge il vincolo, ma anche il luogo nel quale sorgono le eventuali obbligazioni a carico delle parti, esso sarà il luogo in cui si trova il server di posta del destinatario. Tale effetto - collegato alla deroga del principio della conoscenza contenuto nell'art. 1335 c.c. (Fragali*, in Commentario a cura di D'Amelio e Finzi, Obbligazioni, I Firenze, 1948,* pp. 352-353) - può portare, per le caratteristiche della Rete, a conseguenze sul piano pratico a dir poco singolari. Infatti - anche se non vi sono problemi nell'individuazione della giurisdizione (fissata dalla Convenzione di Bruxelles – in mancanza di espressa scelta – nel domicilio del convenuto per il business to business e nel domicilio del consumatore per il business to consumer), né dalla legge applicabile (quella del Paese con il quale il contratto presenta il collegamento più stretto, secondo la Convenzione di Roma, espressamente richiamata dalla legge 218/1995) – sanno determinati in base al luogo della conclusione del contratto sia il foro facoltativo per le cause relative ai diritti di obbligazione nascenti dal contratto, previsto dall'art. 20 c.p.c. che gli usi interpretativi ex articolo 1368 c.c., secondo il quale "le clausole ambigue s'interpretano secondo ciò che si pratica generalmente nel luogo in cui il contratto è stato concluso". Cfr Tomassi - *Commercio elettronico* - su http://www.interlex.it. A diverse conclusioni, a mio avviso, non condivisibili giunge Claudio Monteleone in *"La conclusione di un contratto online."* - 26/02/2001 su http://www.netjus.org/pages/pagex.asp?article=56

[17] Cosi, fra le altre, Cassazione civile sez. II, 24 ottobre 1998, n. 10564 Napoli c. Cond. P.tta Due Palme n. 6 Palermo Riv. giur. edilizia 1999,I, 445 nota (GRONDONA); Cassazione civile, sez. lav., 27 gennaio 1988 n. 715, Rusciano c. Societa' Alfa Romeo, Giust. civ. Mass. 1988, fasc. 1, la quale cita come conformi anche le sent. nn. 2457-68 e 629-78.

[18];

- in base alla norma in esame, per indirizzo deve intendersi un luogo, che - per collegamento ordinario o normale frequenza o preventiva indicazione - appartenga alla sfera di dominio o controllo del destinatario[19].

Mentre i primi due principi possono ben convivere con il sistema di trasmissione di un documento informatico mediante posta elettronica, come regolato dall'art. 14 T.U. 445/2000, il terzo suscita serie perplessità.

Un "indirizzo di posta elettronica" – che l'art. 22 lett. h) del DPR 445/2000 definisce come l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici - non può, per le caratteristiche tecniche del sistema sopra esaminate, considerarsi come appartenente alla "sfera di dominio o controllo del destinatario". Per ragioni intuitive, questi non potrà mai avere sul " proprio server" di posta in arrivo le stesse possibilità di governo e vigilanza esercitabili nel luogo in cui vive e/o lavora, in quanto nel normale sistema di posta elettronica è sempre e necessariamente coinvolto un terzo, sulla cui affidabilità è lecito nutrire qualche dubbio[20].

Ma vi è di più. Si pensi, per esempio, al caso in cui la trasmissione del messaggio sia resa impossibile dal fatto che la casella di destinazione piena. Evento questo, che il servizio di posta certificata – che esamineremo in seguito – documenta inviando al mittente un messaggio di notifica dell'errore, che prova da un lato l'omessa consegna e dall'altro che l'inoltro è stato effettuato. Orbene, in tale ipotesi il documento trasmesso a tale indirizzo potrà considerarsi come inviato e pervenuto al destinatario? Una risposta positiva ci sembra inaccettabile, perché nel caso di specie non può individuarsi una "trasmissione", ma solo un "tentativo" non andato a buon fine. Peraltro, non può

---

[18] Così Cassazione civile, sez. III, 3 ottobre 1985 n. 4783, Montesu c. Angelini, Giust. civ. Mass. 1985, fasc. 10; Cassazione civile, sez. lav., 27 gennaio 1988 n. 715, Rusciano c. Societa' Alfa Romeo, Giust. civ. Mass. 1988, fasc. 1, che cita come conformi le sentenze della S.C. nn. 450-85, 2082-72

[19] Cassazione civile sez. lav., 13 dicembre 2000, n. 15696 Petrillo c. Fiat auto Giust. civ. Mass. 2000,2588; Cassazione civile sez. II, 24 ottobre 1998, n. 10564 Napoli c. Cond. P.tta Due Palme n. 6 Palermo Riv. giur. edilizia 1999,I, 445 nota (GRONDONA); Cassazione civile sez. lav., 30 marzo 1992, n. 3908 Soc. Fincantieri c. Cacciola Nuova giur. civ. commentata 1993,I, 345 nota (TRAVERSO); Cassazione civile, sez. III, 9 settembre 1978 n. 4083, Ist. b. S. Paolo Torino c. Soc. S.a.l.c.e., Foro it. 1979, I,400

[20] Tale notoria circostanza trova conferma nelle condizioni generali di contratto, che regolano la maggior parte dei rapporti

La nota continua alla pagina successiva

escludersi che il destinatario debba rispondere dei danni, se l'impossibilità della trasmissione del documento fosse imputabile al suo comportamento negligente, consistito nel non aver cancellato i vecchi messaggi già letti. Comportamento negligente, che - come è noto – è una causa possibile ma non necessaria dell'evento in esame, poiché la casella di destinazione potrebbe essere divenuta "incapiente" anche pochi minuti prima della fallita trasmissione a seguito dell'invio allo stesso destinatario – a sua insaputa o anche contro il suo consenso espresso o presunto – di altri documenti di grande dimensione. Secondo quali parametri dovrà, quindi, valutarsi la diligenza del titolare di un indirizzo di posta elettronica? E come potrà egli provare l'assenza di colpa? Problemi questi, evidentemente sconosciuti all'invio della dichiarazione presso un indirizzo inteso come luogo fisico.

Una semplicistica ed acritica equiparazione delle nozioni di indirizzo, delineate rispettivamente dall'art. 22 lett. h) del DPR 445/2000 e dall'art. 1335 c.c., mi sembra ancor più pericolosa a causa della difficoltà che incontrerebbe il destinatario per superare la presunzione di conoscenza del messaggio, provando l'incolpevole impossibilità di averne avuto notizia[21].

Sempre a tale proposito deve ricordarsi anche che la *cd. presunzione di conoscenza* si estende, oltre che alla mera cognizione, anche all'esatta cognizione dell'atto. Il dichiarante dovrà provare che la dichiarazione è esattamente pervenuta o che, quanto meno, le eventuali discordanze non siano a lui imputabili e il destinatario dovrà provare che l'erronea percezione non sia a lui imputabile[22]. Supponendo che il primo riesca ad assolvere l'onere probatorio a suo carico, come potrà il destinatario provare che il messaggio di posta gli è pervenuto "corrotto"?

Le perplessità appena espresse mi inducono, quindi, ad auspicare interpretazione quanto mai restrittiva della nozione di "indirizzo elettronico dichiarato" introdotta dal citato art. 14 del T.U. 445/2000.

---

di fornitura del servizio di trasmissione e ricezione di posta elettronica.

[21] Si potrebbe osservare che le difficoltà di prova del destinatario sono in concreto mitigate da quelle che il mittente dovrà affrontare per dimostrare l'invio del messaggio di posta, di cui parlerò in seguito. Ma, il rilievo è solo parzialmente fondato, in quanto mentre il secondo potrebbe assolvere l'onere probatorio a suo carico, depositando i log dei vari MTA coinvolti nella trasmissione – i quali testimoniano l'invio e l'arrivo del messaggio all'indirizzo del destinatario – come potrebbe quest'ultimo provare l'eventuale (ma non improbabile) "perdita" del messaggio, imputabile a terzi o al suo fornitore del sevizio di posta, prima che ne abbia potuto avere notizia?

[22] Mirabelli, Dei contratti in generale, in Commentario del codice civile, UTET, 1980, pag, 102

La sostanziale diversità tra l'indirizzo inteso come luogo, sul quale il destinatario può esercitare la facoltà di dominio o controllo, e quello di posta elettronica impongono, infatti, di interpretare *cum grano salis* la norma in esame.

Così, per esempio, non ritengo possa considerarsi come "indirizzo di posta dichiarato" quello "ricavato" da carta intestata, da un sito WEB, da un biglietto da visita o da un e-mail non recenti[23], a meno che altre circostanze (espressa dichiarazione del destinatario, breve lasso di tempo trascorso tra la consegna - o per gli altri esempi, indicazione, creazione, aggiornamento, trasmissione - di tali documenti e l'invio del messaggio,) non testimonino l'attuale volontà del destinatario di ricevere determinate dichiarazioni presso quella risorsa remota idonea a ricevere e registrare documenti informatici. Perché sia applicabile l'art. 1335, il requisito dell'attualità un indirizzo di posta elettronica mi sembra fondamentale, in considerazione del fatto che questo è molto meno stabile e controllabile di un indirizzo inteso come luogo fisico. È notorio, infatti, che la semplice aggressione da parte di messaggi *spam* o veicoli di virus, può costringerci ad "abbandonare" nel giro di pochi giorni un determinato account di posta, senza che sia possibile dare idonea pubblicità a tale evenienza.[24]

Un'interpretazione restrittiva della nozione di "indirizzo elettronico dichiarato" da me prospettata – oltre ad essere conforme ai principi fissati dalla S.C. in materia di elezione di domicilio[25]

---

[23] Al fine di applicare la presunzione di conoscenza dell'atto recettizio, per indirizzo del destinatario deve invece intendersi qualunque recapito di lui che, in ragione di un collegamento ordinario o di una normale frequenza o di una preventiva indicazione o pattuizione rientri nella sua sfera di dominio e di controllo (nella specie, la cassazione ha ritenuto incensurabile in sede di legittimita' perche' congruamente motivata in fatto, la sentenza d'appello aveva stimato utilmente indirizzata una disdetta contrattuale presso la sede di una societa' della quale il contraente destinatario era amministratore e che risultava dall'intestazione di una lettera con la quale il medesimo aveva inviato pochi giorni prima una comunicazione relativa al contratto). Cassazione civile, sez. III, 9 settembre 1978 n. 4083, Ist. b. S. Paolo Torino c. Soc. S.a.l.c.e., Foro it. 1979, I,400

[24] Si afferma che la "vita media" di un indirizzo di posta elettronica sia di circa due anni. La notizia non è verificabile, ma resta il fatto che vengono commercializzati software, destinati prevalentemente a chi gestisce una newsletter, i quali hanno l'unica funzione di controllare che gli indirizzi di posta contenuti nella "rubrica" siano in quel momento attivo e, quindi, consentono di aggiornare facilmente un indirizzario.

[25] L'atto di elezione di domicilio speciale, che ha, come funzione, la sostituzione, per l'affare in questione, di tutti gli altri parametri di individuazione spaziale della persona (residenza, dimora, domicilio generale) con il luogo specificamente indicato, e, come conseguenza, il dipanarsi degli effetti di cui all'art. 141 c.p.c., deve connotarsi secondo caratteri di incontroversa univocita', onde desumerne la chiara volonta' della parte di riferirsi al luogo prescelto come destinazione non fungibile di tutti gli atti del processo che la riguardino. Non riveste, pertanto, tale carattere quella dichiarazione che si limiti, nel corso delle trattative extraprocessuali per il componimento di una vertenza insorta tra le parti, al semplice invito, rivolto alla controparte, a rivolgersi al proprio legale (con contestuale indicazione dell'indirizzo del medesimo), onde trasferire il livello delle trattative dal piano dei rapporti personali a quello, formale, che presupponga l'assistenza di un avvocato (nella

La nota continua alla pagina successiva

- è altresì coerente con le norme contenute nel Decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 (Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti) in materia di comunicazioni e notificazioni per via telematica[26].

Al riguardo ritengo particolarmente illuminante la lettura della relazione illustrativa di tale provvedimento nella parte dedicata alle comunicazioni ed alle notificazione, ove chiarisce che - mentre per il difensore e per gli esperti e gli ausiliari del giudice si farà riferimento rispettivamente all'indirizzo di posta comunicato dal medesimo al Consiglio dell'ordine (da quest'ultimo reso disponibile agli uffici giudiziari e al pubblico) e a quello comunicato dai medesimi ai propri ordini professionali o all'albo dei consulenti presso il tribunale - per tutti gli altri soggetti l'indirizzo elettronico valido sarà quello dichiarato al certificatore della firma digitale al momento della richiesta di attivazione della procedura informatica di certificazione della firma digitale medesima (comma 2 dell'articolo 7), sempre che il certificatore offra il servizio di rendere disponibile nel certificato l'indirizzo elettronico. Rilievo questo tanto più significativo se si tiene conto, che sempre in detta relazione, si legge che il citato DPR *"intende ... dettare – in una materia non più coperta da riserva di legge - delle norme più specifiche in tema di formazione e trasmissione di documenti informatici con particolare riferimento al processo civile, allo scopo di definire anche nel dettaglio i principi generali*

specie, la S.C., affermando il suindicato principio di diritto, ha cassato senza rinvio la pronuncia del giudice di merito che aveva ritenuto integrante gli estremi di una elezione di domicilio una missiva, indirizzata dal ricorrente alla controparte, del seguente tenore: "per la terra, non voglio parlare con te e nemmeno con il tuo amico: se devi dire qualcosa, il mio indirizzo e' alla via province 21 di Roma dell'avvocato Mindoppi"). Cassazione civile sez. I, 10 novembre 1997, n. 11037 Giust. civ. Mass. 1997,2116

L'elezione di domicilio speciale e' un atto di parte che richiede la forma scritta "ad substantiam" e che non puo' essere surrogata da una comunicazione scritta proveniente dal preteso domiciliatario con la quale si da' atto di una precedente elezione di domicilio. Cassazione civile, sez. I, 8 marzo 1983 n. 1690, Giust. civ. 1984, I,255.

[26] Art. 7 (Indirizzo elettronico)

1. Ai fini delle comunicazioni e delle notificazioni ai sensi dell'articolo 6, l'indirizzo elettronico del difensore è unicamente quello comunicato dal medesimo al Consiglio dell'ordine e da questi reso disponibile ai sensi del comma 3 del presente articolo. Per gli esperti e gli ausiliari del giudice l'indirizzo elettronico è quello comunicato dai medesimi ai propri ordini professionali o all'albo dei consulenti presso il tribunale.

2. Per tutti i soggetti diversi da quelli indicati nel comma 1 l'indirizzo elettronico è quello dichiarato al certificatore della firma digitale al momento della richiesta di attivazione della procedura informatica di certificazione della firma digitale medesima, ove reso disponibile nel certificato.

3. Gli indirizzi elettronici di cui al comma 1, comunicati tempestivamente dagli ordini professionali al Ministero della giustizia, nonché quelli degli uffici giudiziari e degli uffici notifiche (UNEP), sono consultabili anche in via telematica

La nota continua alla pagina successiva

già affermati dal d.P.R. 513/1997, in tema di formazione, archiviazione e la trasmissione (e notificazione) di documenti con strumenti informatici e telematici."

D'altronde, particolare attenzione nell'individuazione dell'indirizzo di posta elettronica presso il quale devono essere trasmessi i documenti informatici, è presente anche nei seguenti provvedimenti:

- Circolare del Ministero delle attività produttive 29 novembre 2002, n. 3553/C - Prime indicazioni attuative dell'art. 31,comma 2,della legge 24 novembre 2000, n. 340 così come modificato dall'art. 3, comma 13, della legge 28 dicembre 2001, n. 448[27];
- Ministero delle attività produttive - Decreto 12 novembre 2001 - Modalità per la presentazione per via telematica o su supporto informatico degli atti di conversione in euro del capitale delle società al fine del deposito per l'iscrizione nel registro delle imprese[28]
- Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 [29].

secondo le modalità operative stabilite dal decreto di cui all'articolo 3, comma 3.

[27] Circolare del Ministero delle attività produttive 29 novembre 2002, n. 3553/C - Prime indicazioni attuative dell'art. 31,comma 2,della legge 24 novembre 2000, n. 340 così come modificato dall'art. 3, comma 13, della legge 28 dicembre 2001, n. 448

[…] Modalità di presentazione: - a) per via telematica
A seguito dell'assegnazione del numero di protocollo, l'ufficio invia telematicamente, la ricevuta del protocollo presso l'indirizzo di posta elettronica registrato all'atto dell'abilitazione al sistema o della trasmissione. […]

[28] Ministero delle attività produttive - Decreto 12 novembre 2001 - Modalità per la presentazione per via telematica o su supporto informatico degli atti di conversione in euro del capitale delle società al fine del deposito per l'iscrizione nel registro delle imprese
[…]A seguito dell'avvenuta iscrizione, al soggetto che ha eseguito il deposito sarà inviata telematicamente la visura aggiornata dei dati risultanti dal registro delle imprese, presso l'indirizzo di posta elettronica registrato. […]

[29] Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428

Art. 12 - Informazioni sulle amministrazioni e le aree organizzative omogenee
1. Ciascuna pubblica amministrazione di cui al decreto n. 29/1993 che intenda trasmettere documenti informatici soggetti alla registrazione di protocollo deve accreditarsi presso l'indice di cui all'art. 11 del presente decreto fornendo almeno le seguenti informazioni identificative relative alla amministrazione stessa:
[…] c) indirizzo della sede principale della amministrazione; […]
2. L'elenco di cui al comma 1, lettera d), comprende, per ciascuna area organizzativa omogenea:

La nota continua alla pagina successiva

In definitiva, ritengo ragionevole affermare che per "indirizzo di posta dichiarato" debba intendersi esclusivamente quello indicato in modo inequivocabile dal destinatario – e sempre che al momento della trasmissione nulla faccia legittimamente supporre che esso non sia più attuale – ovvero quello dichiarato ad un soggetto terzo qual è il Certificatore di firma digitale e da questo reso pubblico. Solo in quest'ultima ipotesi, una certa "solennità" della dichiarazione, da un lato, e la possibilità di rendere pubblica eventuali modificazioni del proprio indirizzo di posta, dall'altro, autorizzano a ritenere che il principio del legittimo affidamento del terzo possa legittimamente prevalga sull'interesse del destinatario alla ricezione di un documento informatico presso il suo effettivo indirizzo di posta elettronica.

[…]c) a casella di posta elettronica dell'area prevista dall'art. 15, comma 3 del presente decreto; […]

Art. 14 - Modalità di aggiornamento dell'indice delle amministrazioni
[…] 3. Ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti. L'indirizzo di tale casella è riportato nell'indice delle amministrazioni pubbliche.
4. I messaggi di posta elettronica ricevuti da una amministrazione che sono soggetti alla registrazione di protocollo, vengono indirizzati, preferibilmente, alla casella di posta elettronica della area organizzativa omogenea destinataria del messaggio.

Art. 15 - Modalità di trasmissione e registrazione dei documenti informatici
[…] 3. Ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti. L'indirizzo di tale casella è riportato nell'indice delle amministrazioni pubbliche.
4. I messaggi di posta elettronica ricevuti da una amministrazione che sono soggetti alla registrazione di protocollo, vengono indirizzati, preferibilmente, alla casella di posta elettronica della area organizzativa omogenea destinataria del messaggio.

Il problema della prova della trasmissione del documento mediante lo strumento della posta elettronica

A tale proposito, dobbiamo innanzitutto precisare che accanto alla normale posta elettronica – il cui meccanismo abbiamo sopra esaminato – esiste e comincia a diffondersi anche quella cosiddetta "certificata"[30].

Il sistema di trasmissione della seconda presenta, rispetto alla prima, significative differenze tecniche, che naturalmente si riflettono anche sul problema della prova dell'invio del messaggio.

Conseguentemente, riteniamo opportuno esaminare la questione con riferimento prima alla normale posta elettronica e poi a quella certificata.

1.1.5 La prova dell'invio di un messaggio con il sistema ordinario di posta elettronica

Come si è già detto a proposito delle caratteristiche tecniche del sistema di trasmissione della posta elettronica, entrambi i tipi di sottosistemi (Mail User Agent *(MUA)* e Mail Transport Agent *(MTA)*) coinvolti nell'invio di un messaggio tengono traccia della loro attività. Le informazioni presenti nel MUA del mittente sono in genere molto povere; maggiori notizie sul percorso seguito dal messaggio sono invece a disposizione del destinatario (nelle cd. intestazioni); gli MTA impegnati nella trasmissione documentano, poi, le operazioni svolte in file denominati log.

L'analisi congiunta – sempre che sia materialmente possibile – delle informazioni generate dai MUA e degli MTA consente in genere di ricostruire con sufficiente precisione la sorte ed il percorso di un messaggio di posta elettronica.

---

[30] Lista degli operatori di posta certificata i cui servizi hanno superato i test di interoperabilità aggiornata al 5.12.03

EDS PA s.p.a.

I.T. Telecom S.p.A

Postecom S.p.A.

ACTALIS S.p.A

Intesa S.p.A

ESANET s.r.l.

EDS Electronic Data Systems Italia S.p.A.

Il problema è dato - più che dalla natura e dall'intrinseco valore probatorio di tali documenti – dal loro effettivo grado di resistenza in un eventuale giudizio che verta sul corretto invio di un documento elettronico all'indirizzo dichiarato dal destinatario.

Infatti, sotto il primo profilo, è che evidente alcun dubbio può nutrirsi sulla natura giuridica dei documenti che rappresentano tali informazioni: essi sono documenti informatici privi di qualsiasi firma elettronica, la cui efficacia probatoria e' quella prevista dall'art. 2712 c.c.[31].

Per quanto riguarda, invece, il secondo - in mancanza di pronunce che abbiano definito giudizi in cui si discuteva della questione che ci occupa - possono trarsi indicazioni utili, sia per la sua soluzione, che per formulare ragionevoli previsioni sul futuro orientamento giurisprudenziale, dallo studio delle sentenze emesse sul valore probatorio del fax e del telex - i quali pur con le note significative differenze sono comunque mezzi che realizzano la trasmissione di documenti – nonché da quelle che hanno affrontato i problemi dell'efficacia riproduzioni meccaniche.

Per quanto riguarda le prime, devo rilevare che quelle da me esaminate sono discordanti[32] e

---

[31] Art. 2712 Riproduzioni meccaniche - Le riproduzioni fotografiche o cinematografiche, le registrazioni fotografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

[32] Considerano la trasmissione a mezzo fax come inidonea a garantire la provenienza di essa dal soggetto legittimato e la sua conformità all'originale, traendone le necessarie conseguenze le seguenti pronunce:

Cassazione penale sez. II, 19 ottobre 1999, n. 12623 Sforza Cass. pen. 2000,2659 (s.m.) Giust. pen. 2000,III, 597 (s.m.)

Cassazione penale sez. V, 5 marzo 1999, n. 4414 Radicchio Riv. cancellerie 1999, 599

Cassazione penale sez. I, 11 maggio 1998, n. 6528 Sileno Cass. pen. 1999,3490 (s.m.)

Cassazione penale sez. VI, 9 marzo 1998, n. 883 Todaro Cass. pen. 1999,2248 (s.m.) Giust. pen. 1999,III, 435

Cassazione penale sez. II, 4 dicembre 1997, n. 243 Maltacesare Cass. pen. 1999, 197 (s.m.)

Cassazione penale sez. I, 25 settembre 1997, n. 5292 Vicino Cass. pen. 1998,2065 (s.m.) Giust. pen. 1998,III, 502 (s.m.)

Corte appello Milano, 2 febbraio 1996 Soc. C.B.I. Factor c. Soc. Conavi Coltiva e altro Dir. fall. 1996,II,1091 nota (D'ATTILIO)

Cassazione penale sez. III, 14 dicembre 1994 Bossalini Cass. pen. 1996,2318 (s.m.)

Viceversa, ignorano del tutto tali problemi le seguenti sentenze:

T.A.R. Toscana sez. II, 12 maggio 2001, n. 826 Benedetti c. Com Bagno Ripoli Foro amm. 2001 (s.m.)

Cassazione penale sez. I, 25 ottobre 2000, n. 6106 D'Ascia Ced Cassazione 2001,RV218185

Cassazione penale sez. I, 11 marzo 1999, n. 2032 Zappia Cass. pen. 2000,2058 (s.m.) Giust. pen. 2000,III, 124 (s.m.)

La nota continua alla pagina successiva

sembrano dettate più da esigenze contingenti, che da un'analisi approfondita dei dubbi, che la trasmissione del documento mediante macchina-fax legittima, in ordine sia alla sua provenienza che alla reale volontà dell'estensore di inviare il documento.

Più utile ai fini che ci occupano, è l'esame della giurisprudenza in materia di riproduzioni meccaniche, la quale è concorde nell'affermare il seguente principio.

Per le riproduzioni fotografiche o cinematografiche, le registrazioni fonografiche e, in genere, rappresentazione meccanica di fatti e di cose, il disconoscimento della loro conformità ai fatti rappresentati non ha gli stessi effetti del disconoscimento della scrittura privata, previsto dall'art. 215, comma 2, c.p.c., perché, mentre quest'ultimo, in mancanza di richiesta di verificazione e di esito positivo di questa, preclude l'utilizzazione della scrittura, il primo non impedisce che il giudice possa accertare la conformità all'originale anche attraverso altri mezzi di prova, comprese le presunzioni[33].

Il disconoscimento, quindi, impedisce solo che il documento faccia piena prova dei fatti e delle cose rappresentate, ma non lo pone nel nulla. Così, per esempio, assume valore ai fini della sua valutazione ogni altro elemento e tra questi, anche la linea difensiva adottata dalla parte che disconosce il documento[34].

Cassazione penale sez. VI, 26 maggio 1997, n. 2136 Adekunle Cass. pen. 1998, 125

Cass. civile sez. I, 29.9.1999, n. 10788 Fall. soc. Le Francois c. Credito agr. bresciano Foro it. 2000,I, 825 Fallimento 2000,1236 nota (TERENGHI) -Conforme- App. Milano, 18.1.2000 Fall. soc. Cogese c. Soc. Thomson Microelectronics e altro

Tribunale Napoli, 15 luglio 1998 Sekavin Enterprises S.A. c. Black Sea Shipping Co. Dir. maritt. 1999, 860

[33] Così, in particolare, Cassazione civile sez. lav., 6 settembre 2001, n. 11445 Torrieri c. Soc. Autostrade Giust. civ. 2001,I,2330 Dir. informatica 2001, 910. Conf. Cassazione civile sez. I, 13 maggio 1992 n. 5662, Messina e altro c. Messina, Giust. civ. Mass. 1992, fasc. 5 Dir. famiglia 1992, 1016.

[34] Cfr. Cassazione civile sez. lav., 8 luglio 1994, n. 6437 Soc. Savi trasp. c. Rossi Orient. giur. lav. 1994, 827 Arch. giur. circol. e sinistri 1995, 151 Riv. it. dir. lav. 1995,II, 447 nota (VALLEBONA). Nella motivazione della sentenza (che affrontava, tra l'altro, il valore probatorio dei dischi cronotachigrafi ritualmente disconosciuti) si legge testualmente […] l'avvenuto disconoscimento nel senso che precede […] atteso che esso non inficia del tutto la portata probatoria di tali meccanismi, ma la degrada a livello di mera, contestata "praesumptio iuris tantum" o semplice, ne risulta con evidenza che l'indagine dei giudici di merito doveva essere orientata nel senso di accertare se e con quali ulteriori mezzi il ricorrente avesse ottemperato, in via integrativa, all'"onus probandi" che su di lui incombeva. Tale prova, appunto poiche' integrativa e di supporto, in quanto rivolta a superare l'elemento ostativo del disconoscimento della valenza dei dispositivi menzionati, puo' essere offerta o ricavata, anche a mezzo di ulteriori presunzioni semplici, senza che cio' importi una inversione del principio fissato dall'art. 2697 Cod. Civile, quale la circostanza che la S.A.V.I., nel corso dei tre gradi del giudizio, non si e' mai peritata di produrre gli originali cronotachigrafi, con i relativi dischi registrati, certamente in suo possesso per l'obbligo di conservazione annuale a lei facente carico, ne', sintomaticamente, ha mai indicato nelle sue difese il contenuto,

La nota continua alla pagina successiva

Interessante a questo proposito, appare una recente sentenza della S.C. (Cassazione Civile, sez. III, 28 gennaio 2003, n.1236), la quale – decidendo un ricorso della Telecom contro una sentenza della Corte di Appello di Napoli che aveva ordinato alla società telefonica di ripristinare l'utenza telefonica disattivata per il mancato pagamento di due bollette – conferma gli stessi principi, precisando inoltre che "*[...] se il buon funzionamento sia contestato anche mediante richiesta di un accertamento tecnico sulla funzionalità dell'impianto di contabilizzazione, costituisce onere della società esercente il servizio di telefonia offrire la prova dell'affidabilità dei valori registrati da contatori funzionanti. Anche in tal caso l'utente è ammesso a provare che non gli sono addebitati gli scatti risultanti dalla corretta lettura del contatore funzionante, mediante l'allegazione di circostanze che univocamente autorizzino la presunzione di un'utilizzazione esterna della linea nel periodo al quale gli addebiti si riferiscono. A tale fine non è tuttavia sufficiente che il traffico telefonico appaia straordinario rispetto ai livelli normali, ovvero che si sia svolto verso destinazioni inusuali, o in assenza dell'utente, ma è necessario che possa ragionevolmente escludersi anche che soggetti diversi dal titolare dell'utenza abbiano fatto un uso abnorme del telefono per ragioni ricollegabili ad un difetto di vigilanza, ovvero alla mancata adozione di possibili cautele da parte dell'intestatario.[...]*[35].

Sulla base di tali precedenti è, quindi, difficile prevedere l'esito di un giudizio nel quale si discuta della fedele trasmissione di un documento informatico mediante il servizio di normale posta elettronica.

Colui il quale allegherà l'invio e la corretta ricezione, dovrà far acquisire agli atti del processo i log degli MTA coinvolti nella trasmissione e – nel caso in cui, come è prevedibile, la controparte ne disconosca la conformità ai fatti documentati – l'esame si sposterà sull'affidabilità delle

---

eventualmente diverso, da quello risultante dalle fotocopie ex adverso esibite, al fine di dimostrare la reale entita' delle ore lavorative effettuate dal Rossi, limitandosi soltanto ad una generica contestazione dello straordinario vantato dall'altra parte e della portata probatoria degli apparecchi cronotachigrafi. Ne' puo' essere del tutto obliterata la valenza ausiliaria di eventuali ammissioni stragiudiziali effettuate dalla parte resistente in precedenza, sia pure in circostanze e per motivi diversi, ma comunque sempre pertinenti ai fatti di causa, quale, nella specie, il generico riconoscimento dello straordinario ad opera della S.A.V.I. nell'accordo sindacale intervenuto tra la stessa ed i suoi dipendenti, tra cui il Rossi (che, tuttavia, non lo sottoscrisse ritenendolo lesivo dei suoi diritti), in data 8.10.1988 (doc. n. 10 del fascicolo di parte), nel quale l'azienda si impegnava a versare agli autisti un compenso forfettario per lo straordinario effettuato; documento, questo, mai contestato, ed anzi del tutto ignorato nelle sue difese dalla resistente, malgrado reiterati, espliciti riferimenti allo stesso da parte del ricorrente a titolo di ulteriore riprova del fondamento del diritto vantato. […]

Conf. Cassazione civile sez. lav., 20 dicembre 2001, n. 16098 Speziali c. Soc. Martinelli trasp. Giust. civ. Mass. 2001,2190

[35] Conf. Cassazione civile sez. III, 10 settembre 1997, n. 8901 Soc. Sip c. Mura Foro amm. 1998,1007

macchine e dei loro gestori e su tutte le altre circostanze che possano univocamente portare a confermare od escludere il loro buon funzionamento, ovvero gli altri fatti rispettivamente allegati dalle parti a sostegno delle proprie pretese.

1.1.6 La prova dell'invio di un messaggio con il sistema ordinario di posta elettronica certificata

Fin qui ho affrontato i problemi collegati alla prova dell'invio e della ricezione di un documento informatico trasmesso mediante il normale sistema di posta elettronica .

Ma, come si è accennato, cominciano a diffondersi servizi di cd. posta elettronica certificata, i quali si differenziano da quella ordinaria per alcune significative caratteristiche tecniche, che si riflettono sulla disciplina giuridica della prova della trasmissione .

La regolamentazione fondamentale di tale servizio è descritta nelle "Linee Guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata", emesso in data 3.2.2003 dal Centro Tecnico per la Rete Unitaria della P.A. Area Rete Unitaria ed approvate con Decreto della Presidenza del consiglio dei ministri 14 ottobre 2003, nonché dal relativo allegato tecnico – giunto alla terza edizione del 29.5.03 - che descrive le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata.

1.1.6.1 Gli aspetti tecnici della cd. posta certificata

Anche per tale servizio di messaggistica - e dei problemi giuridici che pone – seguirò il metodo di esposizione usato per la posta elettronica normale: esaminerò preliminarmente gli aspetti tecnici.

In buona sostanza, il messaggio di posta certificata nel "tragitto" dal mittente al destinatario viene elaborato così dai gestori della posta elettronica certificata:

1. Allorché il punto d'accesso[36] del gestore di posta certificata del mittente riceve un messaggio da spedire, fa qualche controllo[37] sul medesimo e – in mancanza di problemi[38] invia al

[36] È il punto che fornisce i servizi di accesso per l'invio di messaggi di posta certificata. Il punto di accesso fornisce i servizi di accesso dell'utente, emissione della ricevuta di accettazione, imbustamento del messaggio originale nel messaggio di trasporto. Così, Allegato tecnico citato

[37] Al momento dell'accettazione del messaggio il punto di accesso deve garantirne la correttezza formale verificando che:

nel corpo del messaggio esista un campo "To" riportante uno o più indirizzi email conformi alle specifiche RFC 2822 §3.4.1;

l'indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato

La nota continua alla pagina successiva

mittente una ricevuta di accettazione[39], firmata digitalmente, in cui indica quali sono i destinatari che appartengono alla posta certificata e quali sono quelli esterni; la ricevuta contiene la data e l'ora di elaborazione (data e ora di invio) e deve, naturalmente, essere conservata dal mittente.

2. Lo stesso gestore provvede, quindi, a imbustare il messaggio originale[40] del mittente in un "messaggio di trasporto"[41] e lo invia al server di destinazione (o, punto di ricezione)[42].

3. Questo dovrà effettuare esclusivamente dei controlli formali sul messaggio ricevuto, all'esito positivo dei quali, inoltrerà il messaggio di trasporto immodificato[43] al punto di consegna e, al tempo stesso, una ricevuta di presa in carico[44] al gestore mittente[45], al fine di consentire il

---

nel campo "From" del messaggio;

gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) siano presenti nei campi "To" o "cc" del messaggio.

Così, Allegato tecnico citato

[38] Qualora il messaggio non fosse formalmente valido, il punto di accesso dovrà non accettare il messaggio all'interno del sistema di posta certificata non emettendo, quindi, la relativa ricevuta di accettazione. Così, Allegato tecnico citato

[39] È la ricevuta, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta certificata. La ricevuta di accettazione è firmata con la chiave del gestore di posta certificata del mittente. Così, Allegato tecnico citato

[40] È il messaggio originale inviato da un utente di posta certificata prima del suo arrivo al punto di accesso. Il messaggio originale è consegnato all'utente di posta certificata di destinazione per mezzo di un messaggio di trasporto che lo contiene. Così, Allegato tecnico citato

[41] È il messaggio creato dal punto di accesso, all'interno del quale è inserito il messaggio originale inviato dall'utente di posta certificata ed i relativi dati di certificazione. Il messaggio di trasporto è firmato con la chiave del gestore di posta certificata mittente. Il messaggio di trasporto è consegnato immodificato nella casella di posta certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente. Così, Allegato tecnico citato

[42] Punto di ricezione - È l'entità che riceve il messaggio all'interno di un dominio di posta certificata. Corrisponde alla macchina destinata alla ricezione dei messaggi per il dominio. Effettua i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in un messaggio di anomalia di trasporto. Così, Allegato tecnico citato

[43] Il citato allegato chiarisce che tale soluzione presenta il seguente vantaggio rispetto ad una soluzione che prevede la ritrasformazione del messaggio di trasporto nel messaggio originario: si ottiene la visibilità dei dati di certificazione inseriti dal messaggio (testo, XML, ulteriori allegati) permettendone così la verifica da parte del destinatario.

[44] È emessa dal punto di ricezione verso il gestore di posta certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del dominio di posta certificata di destinazione. Nella ricevuta di presa in carico sono inseriti i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce. Così, Allegato tecnico citato

[45] Più precisamente, il punto di ricezione, a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:

La nota continua alla pagina successiva

tracciamento del messaggio nel passaggio tra un gestore ed un altro.

4. All'arrivo del messaggio presso il punto di consegna[46], il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta di avvenuta consegna mittente. Questa è emessa esclusivamente a fronte della ricezione di un messaggio di trasporto valido. In tutti gli altri casi (es. messaggi di anomalia di trasporto), la ricevuta di avvenuta consegna non è emessa. In ogni caso, il messaggio ricevuto dal punto di consegna deve essere consegnato immodificato alla casella di posta del destinatario. La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente ed un allegato XML con i dati di certificazione in formato elaborabile oltre ad eventuali allegati per funzionalità aggiuntive offerte dal gestore. Se il messaggio pervenuto al punto di consegna non fosse recapitabile alla casella di destinazione (se, per esempio, la casella fosse piena), il punto di consegna emetterebbe una ricevuta di errore di consegna. La ricevuta di errore di consegna, si badi bene, è generata, a fronte di un errore, esclusivamente nei casi previsti per la ricevuta di avvenuta consegna (ovvero, solo in caso di arrivo di un messaggio di trasporto corretto).

Le operazioni appena descritte – che sono rappresentate nel grafico riportato in appendice[47] - descrivono il percorso di un messaggio tra due soggetti che si appoggiano entrambi ad un gestore di

---

verifica la correttezza/natura del messaggio in ingresso;

se il messaggio in ingresso è un messaggio di trasporto corretto:

emette una ricevuta di presa in carico verso il gestore mittente;

inoltra il messaggio di trasporto verso il punto di consegna (cfr. 2.5);

se il messaggio in ingresso è un messaggio di trasporto errato/non è un messaggio di trasporto:

imbusta il messaggio in arrivo in un messaggio di anomalia di trasporto (cfr. 2.4.3);

inoltra il messaggio di anomalia di trasporto verso il punto di consegna.

Così, Allegato tecnico citato

[46] Punto di consegna - Effettua la consegna del messaggio nella casella di posta elettronica dell'utente di posta certificata destinatario. Verifica la provenienza/correttezza del messaggio, emette la ricevuta di avvenuta consegna. Così, Allegato tecnico citato

[47] il grafico riproduce fedelmente quello riportato nell'Allegato tecnico citato, pag. 27, 8.1.1. Interazione fra due domini di posta certificata

posta certificata. Ma, come si è detto, è possibile che uno dei due (il mittente o il destinatario) rispettivamente invii o riceva il messaggio utilizzando un provider di posta di posta normale.

Esaminiamo, separatamente le due ipotesi, per capire cosa avviene dal punti di vista tecnico.

- *Messaggio da posta normale a posta certificata*

1. L'utente trasmette un messaggio di posta elettronica impegnando un MTA di posta normale ad un indirizzo di posta elettronica gestito da un provider di posta certificata (punto di ricezione)

2. Il punto di ricezione esamina il messaggio e lo riconosce come sprovvisto delle caratteristiche richieste dalle linee guida di posta certificata; conseguentemente, crea un messaggio di anomalia di trasporto[48], firmato digitalmente, a cui allega il messaggio ricevuto. Il messaggio di anomalia viene inoltrato al punto di consegna (se diverso dal punto di ricezione)

3. Il messaggio di anomalia, a cui è allegato il messaggio ricevuto, viene depositato nella casella del destinatario, che potrà accedere alla casella di posta e leggere il messaggio di anomalia che contiene il messaggio originale.

Nell'ipotesi appena esaminata – anch'essa rappresentata in un grafico riportato in appendice - al mittente non viene recapitata alcuna ricevuta di consegna del messaggio.

- *Messaggio da posta certificata a posta normale*

1. Il mittente invia il messaggio al punto di accesso di un gestore di posta certificata, che lo riceve;

2. Il comportamento di tale MTA è identico a quello che adotterebbe per messaggi indirizzati

[48] Messaggio di anomalia di trasporto - Quando un messaggio errato/non di posta certificata deve essere consegnato ad un utente di posta certificata, il messaggio è inserito in un messaggio di anomalia di trasporto per evidenziare l'anomalia al destinatario. Il messaggio di anomalia di trasporto è firmato con la chiave del gestore di posta certificata del destinatario. Così, Allegato tecnico citato

ad un destinatario munito di indirizzo di posta certificata, sicché anche in tal caso fa qualche controllo sul messaggio (gli stessi indicati nella nota 34) e, se non ci sono problemi, invia al mittente una ricevuta di accettazione, firmata digitalmente, in cui indica quali sono i destinatari che appartengono alla posta certificata e quali sono quelli esterni; per questi ultimi la trasmissione non viene considerata di posta certificata. La ricevuta contiene la data e l'ora di elaborazione (data e ora di invio).

3. il punto d'accesso crea, quindi, un messaggio di trasporto (lo stesso indicato nella nota 42) a cui viene allegato il messaggio originale; il messaggio di trasporto contiene alcune informazioni sulla trasmissione, tra cui la data e l'ora di invio. Il messaggio di trasporto viene firmato dal provider mittente e spedito al destinatario.

Naturalmente, nemmeno in quest'ipotesi – rappresentata in un grafico riportato in appendice - il mittente riceverà una ricevuta di consegna del messaggio. Ma questa volta per ragioni diverse da quelle del caso sopra esaminato: in quello il punto di consegna, una volta verificato che il messaggio non perviene da un gestore di posta certificata, considera giustamente questa come un'anomalia (infatti, nel caso in esame manca la necessaria garanzia sul percorso fino ad allora seguito dal documento) e crea un messaggio che segnala la medesima; in questo la ricevuta di consegna del messaggio manca perché non vi è un punto di consegna programmato per crearla ed inviarla.

Prima di chiudere l'esame delle caratteristiche tecniche della posta certificata, deve ricordarsi che il sistema mantiene traccia di tutte le operazioni di trattamento del messaggio in un file log,[49] che il Gestore deve conservare per almeno due anni e rendere disponibile ed accessibile per fini

[49] Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, i gestori devono mantenere traccia delle operazioni svolte su un apposito registro. I dati contenuti nel suddetto registro devono essere conservati per un periodo di almeno due anni e devono essere disponibili ed accessibili per la consultazione a fini ispettivi, da parte del Centro Tecnico, o in caso di contenzioso dai soggetti individuati per tale compito. Per la gestione del registro i gestori devono adottare le soluzioni tecniche e organizzative che garantiscano la riservatezza e la sicurezza (autenticità ed inalterabilità nel tempo) delle informazioni in esso contenute. Così, Allegato tecnico citato

Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi inviati, le informazioni presenti nei registri degli operatori coinvolti nell'invio sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. Così, Linee Guida cit.

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema deve mantenere traccia delle operazioni svolte. Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:

La nota continua alla pagina successiva

ispettivi o in caso di contenzioso. Ciò è particolarmente utile nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi inviati, in quanto – come è espressamente dalla Linee Guida citate - le informazioni presenti nei registri degli operatori coinvolti nell'invio sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

• il codice identificativo univoco del messaggio originale (Message-ID)

• la data e l'ora dell'evento

• il mittente del messaggio originale

• l'oggetto del messaggio originale

• il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)

• il codice identificativo dei messaggi generati (ricevute, errori, ecc.)

• il server mittente

• il server destinatario

Gli effettivi dati registrati sui singoli log dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.). Così, Allegato tecnico citato

1.1.6.2 I problemi giuridici connessi alla cd. posta certificata

La posta elettronica certificata delineata nei documenti sopra citati, in quanto capace di assicurare (*rectius*: documentare) l'avvenuta consegna del documento, fa sì che la trasmissione del documento con tale sistema sia da considerarsi – in virtù dell'art. 14 T.U. 445/2000 - equivalente alla notificazione per mezzo della posta nei casi consentiti per legge.

Deve ritenersi, inoltre, che con il sistema in esame siano realizzate anche le condizioni richieste dal II comma di tale articolo per l'opponibilità ai terzi della data e dell'ora di invio e di ricezione del documento informatico[50].

Come risulta dalla breve descrizione del meccanismo della posta elettronica, l'attendibilità delle informazioni relative all'intero processo di trasmissione si fonda – come per la firma digitale – sulla presenza di terze parti fidate: i gestori del servizio di posta certificata.

Sono essi il punto fermo su cui viene edificato l'intero sistema.

Le linee guida si occupano, quindi di disciplinare l'esercizio dell'attività di gestore di posta certificata – sia da parte delle pubbliche amministrazioni, che dei privati (questi ultimi devono avere natura giuridica di società di capitali) – prevedendo che essa sia condizionata all'inoltro alla Presidenza del Consiglio dei ministri - Dipartimento per l'innovazione e le tecnologie della domanda di iscrizione nell'indice dei gestori di posta certificata.

Nello stesso documento si prevede, inoltre, che i gestori di posta debbano:

a) dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta certificata;

b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze

[50] Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è necessario disporre di un accurato riferimento temporale. Tutti gli eventi (generazione di ricevute, messaggi di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna devono impiegare un unico valore temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, ricevute, messaggi, ecc. generati dal server. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca uno scarto non

La nota continua alla pagina successiva

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, e che sia in grado di rispettare le norme del presente documento e le regole tecniche contenute nell'allegato tecnico;

c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;

d) utilizzare dispositivi e prodotti protetti da alterazioni e che garantiscano la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;

e) adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta certificata;

f) fornire i dati, di cui all'allegato tecnico, necessari per l'iscrizione nell'indice dei gestori.

Si stabilisce, altresì, che il venir meno di uno o più requisiti tra quelli precedentemente indicati comporta la cancellazione dall'elenco e che la Presidenza del Consiglio dei ministri - Dipartimento per l'innovazione e le tecnologie - svolge funzioni di vigilanza e controllo nel settore.

L'altro pilastro che assicura l'attendibilità delle informazioni relative alla trasmissione del documento è costituito dal fatto che buona parte dei documenti informatici creati dalle macchine impegnate dai gestori di posta certificata è firmata con la chiave dei gestori di posta certificata. Tale impiego della crittografia asimmetrica assicura, infatti, la provenienza e l'integrità del documento informatico.

In particolare, sono firmati con tale sistema tutti i messaggi generati dal sistema[51].

---

superiore ad 1 secondo rispetto al Tempo Universale Coordinato (UTC).

[51] […] 6.1 Formato dei messaggi generati dal sistema

Il sistema genera i messaggi (ricevute, messaggi di trasporto e di anomalia di trasporto) in formato MIME. I messaggi sono composti da una parte di testo descrittivo, per l'utente, e da una serie di allegati (messaggio originale, dati di certificazione, ecc.) variabili a seconda della tipologia del messaggio.

Il messaggio (composto dall'insieme delle parti descritte nelle specifiche sezioni del presente allegato) è quindi inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del gestore di posta certificata. Il certificato associato alla chiave usata per la firma deve essere incluso in tale struttura. Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il "multipart/signed" (formato .p7s) così come descritto nella RFC 2633 §3.4.3. […]

La nota continua alla pagina successiva

A proposito di tali documenti, ritengo opportune le seguenti considerazioni.

Per quanto concerne la loro natura, deve rilevarsi che - a dispetto del loro tenore letterale, simile ad una dichiarazione[52] - essi sono da qualificarsi come "documenti narrativi"[53], in quanto non rappresentano dichiarazioni, di volontà o di scienza, di un determinato soggetto, ma dei fatti, ovvero, le operazioni effettuate da una macchina. Più precisamente, esse sono vere e proprie riproduzioni meccaniche di fatti.

Conseguentemente, la loro efficacia probatoria dovrebbe essere quella prevista dall'art. 2712 c.c., con la conseguenza che – in mancanza di disconoscimento - essi fanno piena prova dei fatti rappresentati[54].

[…] Il meccanismo di sicurezza per il colloquio tra i server partecipanti all'infrastruttura di posta certificata è realizzato mediante imbustamento e firma dei messaggi in uscita dal punto di accesso e la loro verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di un messaggio di trasporto. Il messaggio di trasporto firmato permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario. La firma apposta sul messaggio dal sistema mittente è verificata all'arrivo sul server di destinazione. […]

Così, Allegato tecnico citato

[52] Riporto a titolo di esempio il testo di una ricevuta di avvenuta consegna:

Ricevuta di avvenuta consegna

Il messaggio da lei inviato, "prova", è stato consegnato nella casella

destinatario@dominiopostacertificata

dal sistema di posta certificata Legalmail.

Questa ricevuta, per Sua garanzia, è firmata digitalmente.

La preghiamo di conservare questa ricevuta come attestato della consegna nella casella indicata.

Informazioni di dettaglio

Il giorno 05/11/2003 alle ore 19:14:31 (+0100) il messaggio "prova" proveniente da "PERONE LEONARDO <leonardoperone@dominiopostacertificata>" ed indirizzato a:

destinatario@dominiopostacertificata

è stato consegnato nella casella di destinazione.

Identificativo messaggio: B6418708X1068056070128@dominiopostacertificata

[53] GIUSEPPE RANA, Il valore probatorio del documento elettronico; GRAZIOSI, Premesse ad una teoria probatoria del documento informatico, in Riv. trim. dir. proc. civ., 1998, 489.

[54] Sembrano propendere comunque per tale soluzione – anche se in base alla precedente formulazione dell'art. 10 - Manlio Cammarata e Enrico Maccarone, *Il valore probatorio del documento informatico, 01.02.01* -

La nota continua alla pagina successiva

Ma, come si è detto, tali documenti sono anche firmati con la chiave dei gestori di posta certificata. Sorge, quindi, il problema del coordinamento del citato art. 2712 con l'art. 10 del T.U. 445/2000.

Orbene, nonostante il meccanismo di firma utilizzato sia identico a quello impiegato per la firma digitale disciplinata dal predetto T.U.[55], non ritengo che i documenti sopra citati possano considerarsi come sottoscritti con firma digitale, ovvero con una cd. firma elettronica qualificata.

Invero, nel sistema in esame mancano i requisiti di sicurezza previsti per i dispositivi e le procedure per la generazione della firma digitale in senso stretto. Deve, inoltre, rilevarsi che - sia nelle "Linee Guida" che nell'allegato tecnico - nulla si dice in ordine ai tempi di sostituzione delle chiavi private impiegate dai gestori per la cifratura dei documenti in esame. Elemento questo, che non è certo irrilevante ai fini della "robustezza" della firma – poiché, come è noto, più alto è il numero di firme generato e maggiore è il pericolo di rottura del cifrario da parte di esperti decrittatori, dotati di sistemi abbastanza potenti - e che ha, per esempio, ispirato il secondo comma dell'art. 54 DPCM 8.2.99[56].

Ritengo, quindi, che per quanto riguarda l'efficacia probatoria di tali documenti informatici sia quello fissato dal combinato disposto dei commi II e IV[57] dell'art. 10 T.U 445/2000 e non dal III[58].

---

http://www.interlex.it/docdigit/valprob.htm […] Ma un'evidenza informatica può rappresentare qualsiasi altra cosa, come un'immagine, o un suono, o può essere generata automaticamente da un computer (per esempio un file LOG che registra le operazioni compiute dagli utenti di una determinata macchina). Se questa sequenza di bit è provvista di firma digitale sicura, ai sensi del Regolamento, ha il valore probatorio previsto dall'articolo 2712 cc, con tutte le conseguenze processuali derivanti dall'eventuale disconoscimento della parte contro la quale il documento stesso è opposto […

[55] n) FIRMA DIGITALE è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e 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 o di un insieme di documenti informatici;

[56] Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513 - [...] Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale debbono essere sostituite dopo non più di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato. [...]

[57] 2. 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

[….]

La nota continua alla pagina successiva

Applicando le disposizioni appena citate, che ritengo prevalenti su quelle dell'art. 2712 c.c., ciascuno di tali documenti «è liberamente valutabile», sicché - anche in mancanza di disconoscimento – non troverebbe alcuno ostacolo il principio della libera valutazione delle prove e del libero convincimento fissato dall'art. 116 c.p.c..

In realtà, tale conclusione – alquanto paradossale (ma questa è un'altra storia) – non dovrebbe comportare grossi problemi sul piano pratico. Infatti, poiché l'intero sistema sembra comunque assistito da forti caratteristiche oggettive di qualità e sicurezza, ritengo alquanto improbabile che in un eventuale giudizio le risultanze di tali documenti siano ritenute non conformi ai fatti in essi rappresentati.

L'esperienza, poi, si occuperà di confermare o smentire se la fiducia che il legislatore ha mostrato di avere sul costante buon funzionamento delle macchine cui sono affidati i compiti sopra descritti.

Naturalmente, quanto si è appena detto sulla prova della trasmissione di un documento informatico mediante il sistema in esame, vale allorché essa impegni solo domini di posta elettronica certificata.

Infatti, nel caso di interazione tra un dominio di tale tipo ed un altro di posta non certificata, è evidente che non vi è l'ininterrotta catena di certezze, la quale giustifica il forte valore probatorio della trasmissione riconosciuto alla posta certificata, sicché varranno le considerazioni esposte a proposito della posta elettronica ordinaria.

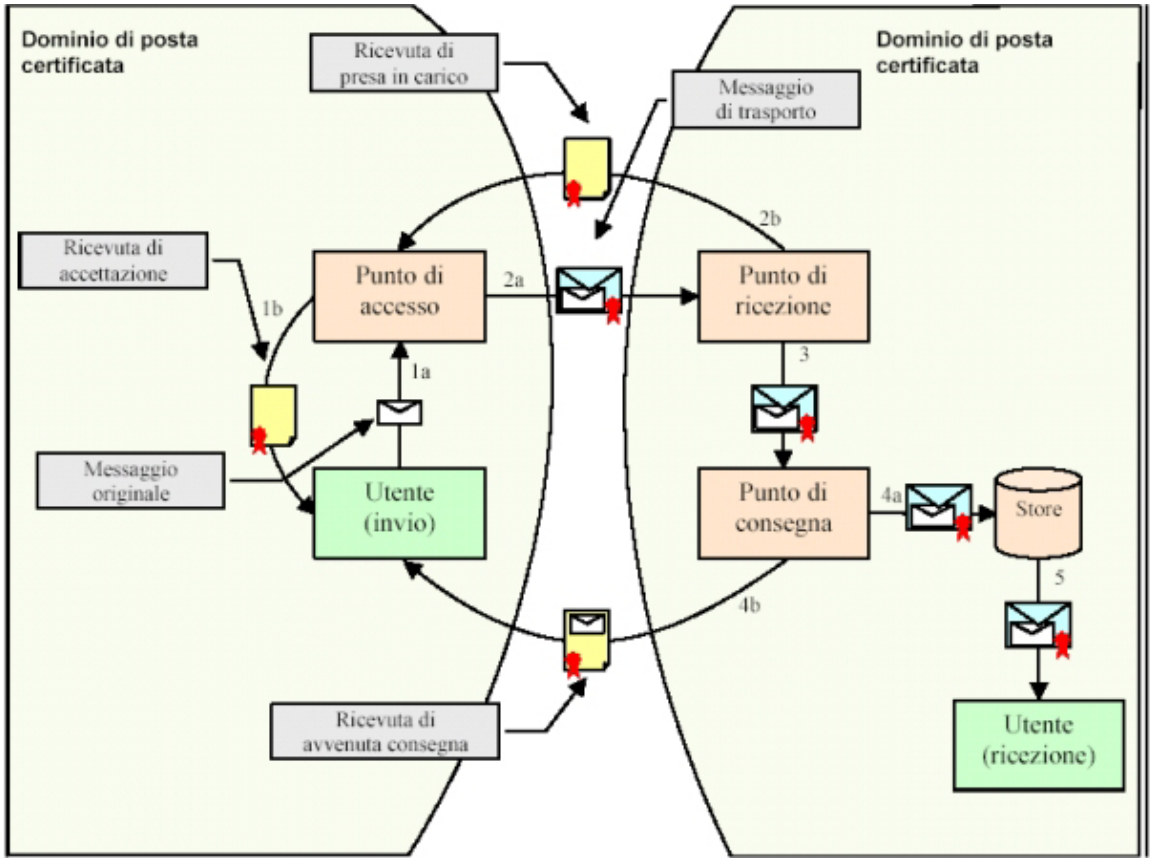
---

4. Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

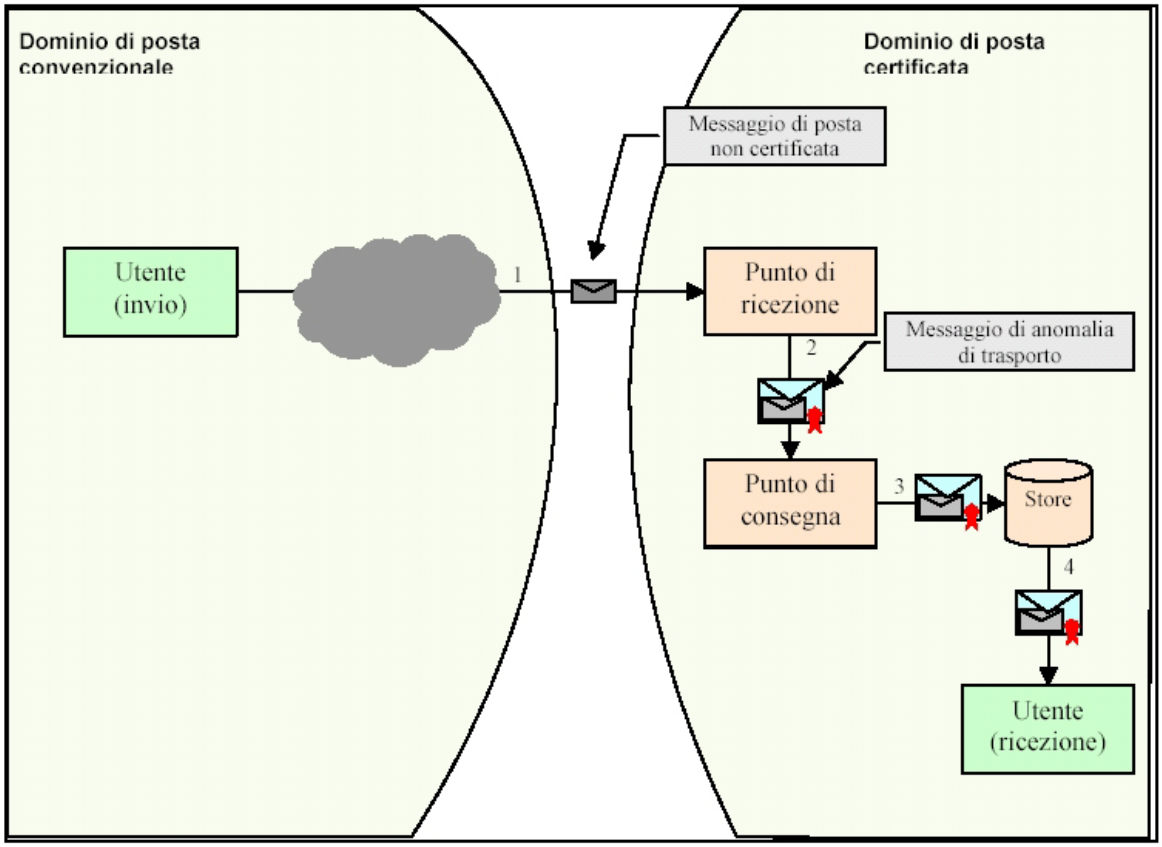
[58] 3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

Appendice A

Rappresentazione grafica delle operazioni svolte su un messaggio di posta che transita da un gestore di posta certificata ad un altro dello stesso tipo



Rappresentazione grafica delle operazioni svolte su un messaggio di posta che transita da un gestore di posta normale ad uno di posta certificata



Rappresentazione grafica delle operazioni svolte su un messaggio di posta che transita da un gestore di posta certificata ad uno di posta normale