

I PROCESSI DI CERTIFICAZIONE NELLA SOTTOSCRIZIONE DEL DOCUMENTO INFORMATICO, NELLA TRASMISSIONE DEI MESSAGGI DI POSTA ELETTRONICA E NEI PROCESSI DI NEGOZIAZIONE TELEMATICA

di Andrea Lisi*

IL PRESENTE SAGGIO COSTITUISCE UNA RIELABORAZIONE DELLA RELAZIONE TENUTA DURANTE IL CONVEGNO “DALLA LEX MERCATORIA ALLA LEX ELECTRONICA NELL’ARCHITETTURA DELL’E-BUSINESS: OPPORTUNITÀ, QUESTIONI LEGALI E TECNOLOGICHE APPLICATE AL MERCATO”, ORGANIZZATO IN DATA 5-6 MAGGIO 2006 DAL CIRCOLO DEI GIURISTI TELEMATICI

VIENE PUBBLICATO SU GENTILE CONCESSIONE DELL’EDITORE NYBERG, POICHÉ GIÀ PUBBLICATO SULLA RIVISTA DI DIRITTO, ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE, N. 2/2007- INFO ALLA PAGINA [HTTP://WWW.NYBERG.IT/RDEGNT/DEFAULT.ASP](http://www.nyberg.it/rdegnt/default.asp)

SOMMARIO:

1. Il contratto ai tempi dell’Internet; 2. Le Firme elettroniche nella vigenza del D. Lgs. 10/2002; 3. Le firme elettroniche nel Codice dell’Amministrazione Digitale (CAD); 4. Cenni alla firma digitale e alla posta elettronica certificata; 5. La “certificazione” del sito web e dei processi di negoziazione

1. Il contratto ai tempi dell’Internet

Attraverso lo scambio di e-mail e la contrattazione “point and click” la Rete consente la formazione di accordi potenzialmente sopranazionali (dove il confine dello spazio e del tempo divengono irrilevanti). Attraverso i siti web di commercio elettronico le manifestazioni del consenso vengono normalmente espresse attraverso la compilazione del formulario *on line* e con il meccanismo del cd. “point and click” (quindi, attraverso la “spuntatura” di una casella¹ e con la digitazione *on line* del tasto negoziale “accetto”). Attraverso il “point&click” qualsiasi manifestazione di consenso o dissenso viene espressa in modo nuovo: dalla semplice manifestazione di consenso al trattamento dei propri dati personali all’accettazione di partecipare ad

* L’avv. Andrea Lisi è titolare dello “STUDIO ASSOCIATO D.&L” (www.studioldl.it), consulenza aziendale e legale per l’e-business e l’international trade. Egli è fondatore del Centro Studi&Ricerche Scint, curatore del portale per l’internazionalizzazione e l’ict www.scint.it e della prima banca dati sul diritto dell’informatica www.scintlex.it. È Direttore della “RIVISTA DI DIRITTO ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE”, Nyberg Editore, Milano e della Collana “DIRITTO, ECONOMIA E SOCIETÀ DELL’INFORMAZIONE”, Cierre Edizioni, Roma. È componente del Comitato Scientifico di varie riviste giuridiche telematiche ed autore di diversi volumi e numerose pubblicazioni in materia di diritto delle nuove tecnologie. È, inoltre, stato docente in master di I e II livello dedicati al diritto dell’informatica, presso l’università di Lecce, Taranto, Padova e Messina e fa parte del Comitato Scientifico del MASTER IN DIRITTO DELL’INFORMATICA E DELL’INFORMAZIONE dell’Università di Messina. E’ attualmente iscritto all’Albo Docenti della Scuola Superiore dell’Amministrazione dell’Interno ed è docente per vari importanti enti di formazione. Egli è, infine, direttore scientifico del corso post lauream di alta formazione in “COMMERCIO ELETTRONICO & INTERNAZIONALE” organizzato da Scint in collaborazione con Ed. Simone e Ipsoa, con il patrocinio del Ministero Attività Produttive e Ice e del Master in Management e Diritto dell’Innovazione Digitale, organizzato dalla Scuola di Formazione Manageriale Aforisma. È arbitro di numerosi enti di risoluzione stragiudiziale delle dispute relative ai domini Internet ccTLD.it e collabora in tutta Italia con università, enti camerali, centri di ricerca, primarie società fornendo progettazione, formazione, assistenza e consulenza legale nell’e-business internazionale, nella privacy, nei servizi di archiviazione ottica/fatturazione elettronica e nel diritto delle nuove tecnologie, in genere.

¹ Un tipico errore in cui incorrono molti titolari di siti web è quello di pre-spuntare le caselle riguardanti la manifestazione di volontà del compratore che, al contrario, andrebbe lasciata in bianco per essere il più libera e trasparente possibile.

un “e-marketplace”, sino alla sottoscrizione di un qualsiasi contratto di compravendita di beni e/o servizi.

È superfluo specificare che il trattamento di dati personali risulta essere un’attività prodromica a qualsiasi successiva operazione di e-commerce: secondo l’art. **23 del Codice della privacy** il trattamento dei dati personali da parte di privati o di enti pubblici economici è ammesso solo con il **consenso espresso** dell'interessato; una volta ricevuta la completa informativa, l'utente del sito web deve, quindi, fornire il suo necessario consenso al trattamento e tale consenso deve essere **documentato per iscritto** (o deve essere **manifestato in forma scritta** in caso di trattamento di dati sensibili).

In primo luogo, pertanto, il consenso non può essere "implicito", cioè non può essere desumibile da comportamenti concludenti. In secondo luogo, deve essere documentato per iscritto (o manifestato in forma scritta in caso di dati sensibili).

E in “forma scritta” vanno anche specificamente sottoscritte le eventuali **clausole vessatorie** presenti in un contratto (<<in ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria>> art. 1341 II comma cod. civ.).

Analogamente deve essere fornita in forma scritta **l’informativa in favore del consumatore nel B2C** (così riportavano sia il decreto legislativo 15 gennaio 1992 n. 50 in materia di contratti negoziati fuori dai locali commerciali, sia il decreto legislativo 22 maggio 1999 n. 185 relativo alla protezione dei consumatori in materia di contratti a distanza, e così oggi è confermato nel Codice del Consumo)².

Adattare tale normativa al web non è cosa ovvia³: la rilevanza e validità del documento elettronico (quale *rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*) e degli stessi contratti telematici effettivamente si può far risalire al 1997 con la **Legge Bassanini** (art. 15 secondo comma L. n. 59/97: *gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*), sino ad arrivare alle piene conferme del **D.P.R. 445/2000** (sostitutivo, come è noto, del D.P.R. 513/1997) e, quindi, alla parziale rivoluzione contenuta nel **Codice dell’Amministrazione Digitale** (D. Lgs. 82/2005, successivamente mod. dal D. Lgs. 159/2006), tanto che oggi si parla della piena validità dei contratti conclusi con strumenti informatici e telematici⁴.

² In verità, oggi la forma scritta ex art. 47 del Codice del Consumo rimane necessaria, ad esempio, in merito all’informazione sul diritto di recesso; mentre secondo l’art. 53 dello stesso Codice le informazioni obbligatorie per il consumatore vanno confermate per iscritto o – a scelta del consumatore – su altro supporto durevole a sua disposizione e a lui accessibile. Il legislatore almeno in quest’ultimo caso ha cercato di risolvere giuridicamente il “problema tecnologico”, anche se molti problemi pur permangono nell’adattare tale regola al web, in quanto secondo la normativa sarebbe il consumatore a dover operare questa scelta e non il titolare del sito...

³ Per un approfondimento della presente problematica si consiglia la lettura del saggio “E-mail e accessi riservati: le nuove norme per la conquista di un’autonoma esistenza giuridica” di A. Lisi, pubblicato nella Rivista di Diritto ed Economia dei Mezzi di Comunicazione, Anno 3 n. 2, 2004, Liguori Editore, p.361 e ss.

⁴ Qualche problema ha suscitato, in passato, l’applicazione dell’art. 11 del D.P.R. n. 513/1997 (riprodotto dal T.U. 445/2000) allorquando sembrava voler garantire efficacia giuridica ai soli contratti conclusi con l’utilizzo della firma digitale. Ma sia l’art. 1322 c.c. sia lo stesso art. 15 della Bassanini rendono certa la piena validità dell’incontro di volontà informatiche, a prescindere se esso sia corredato della firma digitale...L’art. 11 del T.U. n. 445/2000 (ormai abrogato) andava correttamente interpretato: il legislatore con questa norma non aveva voluto assolutamente mettere in dubbio la validità del contratto telematico sprovvisto di firma digitale, ma aveva voluto soltanto sottolineare che

Ma qui il problema preliminare è un altro; e, cioè, se la manifestazione del consenso espressa attraverso la compilazione del formulario on line e, quindi, con il meccanismo del cd. "point and click" (quindi, con la pressione on line del tasto negoziale "accetto") possa essere considerata **comportamento espresso del soggetto** o, invece, vada ritenuto un semplice comportamento concludente, incompatibile con una volontà contraria.

Tenendo conto delle nuove evoluzioni del linguaggio, pare in effetti condivisibile l'opinione di chi ormai considera anche la comunicazione attraverso i "bit" un vero e proprio linguaggio, idoneo a diffondere una precisa volontà contrattuale. La dichiarazione espressa può, infatti, ben manifestarsi anche con segni diversi dalla semplice parola o dalla scrittura, purché tali segni siano sempre riconosciuti e accettati dalla generalità dei consociati come codici di linguaggio, in modo che alle dichiarazioni così effettuate si possa conferire un significato inequivoco di ciò che effettivamente si intende con esse rappresentare. Diversamente qualsiasi odierna acquisizione del consenso al trattamento dei dati personali espressa on line andrebbe ritenuta illegittima perché non in linea con quanto riferito nell'art. 23 del Codice della privacy.

Tale impostazione sembrerebbe peraltro ricevere conferma dalla **Raccomandazione del Gruppo europeo di lavoro per la tutela dei dati personali del 17 maggio 2001**, nella quale si è previsto che il consenso possa essere appunto manifestato "cliccando" su una casella di spunta (quindi, con il meccanismo del "point and click"). Occorre segnalare che anche la più recente **Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002** (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche), nel considerando n. 17), ha precisato che il consenso può essere fornito attraverso qualsiasi modalità idonea a consentire all'utente di esprimere liberamente e consapevolmente i suoi specifici desideri, compresa la selezione di un'apposita casella nel caso di un sito web.

Dunque il consenso elettronico, pur privo di firma digitale, è certamente da considerarsi come valida manifestazione espressa di volontà⁵.

Si può pertanto affermare, che il documento elettronico è certamente una valida manifestazione espressa della propria volontà!

Ma andiamo oltre con l'analisi, ponendoci ulteriori quesiti :

- ✓ *Può il semplice documento informatico considerarsi equivalente al documento scritto?*
- ✓ *Può essere utilizzato per documentare il consenso espresso dell'interessato?*

laddove era prevista dalla legge la forma scritta *ad substantiam* si rendeva assolutamente necessario l'utilizzo della firma digitale. Concetti questi che si ritrovano meglio espressi e ribaditi nel Codice dell'amministrazione digitale.

⁵ Per quanto invece concerne il **contratto concluso per e-mail**, il discorso non cambia di molto, salvo il fatto che l'accordo possa arrivare dopo una anche lunga fase di trattative svoltesi attraverso scambi di posta elettronica. Sul valore formale e probatorio delle e-mail si ricorda che si è animato in Italia un lungo dibattito dottrinale, in seguito all'emissione da parte di una certa giurisprudenza di merito di decreti ingiuntivi basati sulla sola produzione di semplici e-mail (tra i tanti decreti ingiuntivi emessi in quest'ultimo periodo sulla base di una semplice e-mail si ricordano i d.i. del Tribunale di Cuneo pubblicato alla pagina www.scint.it/news_new.php?id=407; del Tribunale di Bari pubblicato alla pagina www.scint.it/news_new.php?id=415; del Tribunale di Mondovì pubblicato alla pagina http://www.scint.it/news_new.php?id=466; del Tribunale di Lucca pubblicato alla pagina www.scint.it/news_new.php?id=484, del Giudice di Pace di Pesaro pubblicato alla pagina www.scint.it/news_new.php?id=499, del Tribunale di Foggia pubblicato alla pagina http://www.scint.it/news_new.php?id=694. L'elenco completo dei provvedimenti giudiziari e dei documenti in linea con tale interpretazione è rintracciabile sul sito web [scint.it](http://www.scint.it)). Dibattito ingiustificato e per certi versi paradossale considerato che una manifestazione di volontà ha un valore giuridico a prescindere dal supporto che la contiene e non c'è ragione alcuna per cui un messaggio di posta elettronica dal contenuto rilevante non possa essere preso in considerazione in un procedimento giudiziario (a maggior ragione se di natura sommaria come il procedimento di emissione di un decreto ingiuntivo).

- ✓ *Può essere utilizzato per la manifestazione scritta della volontà?*
- ✓ *Può essere utilizzato per la specifica sottoscrizione di una clausola vessatoria?*
- ✓ *Può essere utilmente utilizzato per fornire le informazioni scritte in favore dell'utente web/consumatore?*

Il problema non è di poco conto considerato che il consenso scritto per il trattamento dei dati può essere previsto in numerosissimi casi di trattamento dei dati personali sensibili, la documentazione per iscritto è prevista comunque in caso di qualsiasi trattamento di dati, le informazioni obbligatorie per il consumatore vanno inserite in tutti i siti di e-commerce B2C e le clausole vessatorie sono presenti in quasi tutte le condizioni contrattuali presenti sul web!

Per riassumere:

- è corretta quella prassi, ampiamente diffusa tra i titolari dei siti web, di chiedere ai propri utenti di prestare il consenso al trattamento dei dati personali al momento della registrazione al sito web (attraverso il noto meccanismo del cd. "point&click" e, cioè, attraverso la digitazione del tasto virtuale di accettazione delle condizioni contenute nel *form* elettronico), per poter poi successivamente far accedere quello stesso utente ad un'area riservata (normalmente protetta da sistemi di sicurezza e il cui accesso viene garantito da credenziali di autenticazione fornite via e-mail) e, quindi, farlo fruire senza alcuna altra formalità di tutta una serie di servizi (e/o beni) offerti on-line?
- è corretto far sottoscrivere contratti contenenti clausole vessatorie con il sistema del "point & click"?
- è, infine, corretto fornire l'informativa in favore del consumatore semplicemente pubblicandola in un sito web?

Oppure in tutti questi frequentissimi casi occorre utilizzare documenti cartacei e farsi spedire i contratti o le manifestazioni di volontà tramite lettera raccomandata o via telefax?

Se il documento informatico non dovesse, quindi, soddisfare i requisiti della "forma scritta" la maggior parte dei siti web di e-commerce risulterebbero illegittimi!

Per rispondere compiutamente a queste domande e afferrarne la complessità, si dovrebbe affrontare un lungo e confuso excursus legislativo dalla firma digitale (unica tipologia di firma elettronica prevista in Italia dal **D.P.R. 513/1997** e poi dal DPR 445/2000) sino all'avvento delle firme elettroniche cd. "leggere" o "semplici" (considerate per la prima volta dal **Decreto Legislativo n. 10/2002** - attuativo della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche; normativa che aveva modificato il citato D.P.R. n. 445/2000). Ai nostri fini, però, il discorso si rivelerebbe inutile e poco concreto e, quindi, ci limiteremo a verificare brevemente cosa accadeva durante la vigenza del Decreto n. 10/2002 e quali ulteriori innovazioni ha apportato l'entrata in vigore della normativa del **Codice dell'amministrazione Digitale**.

E' opportuno, però, fare delle doverose premesse e specificare cosa si intenda per firma elettronica, per firma elettronica sicura e per firma digitale.

2. Le Firme elettroniche nella vigenza del D. Lgs. 10/2002

Con il termine di “firma elettronica” si suole indicare una qualsiasi tecnica di contrassegno di un documento elettronico, in qualunque forma possibile (anche la semplice indicazione del nome dell’autore in calce al documento)⁶. Quando parliamo di “firme elettroniche sicure o avanzate”, invece, ci riferiamo alle firme che sono in grado di garantire un certo livello di sicurezza e affidabilità al documento sottoscritto, in ordine alla sua provenienza e al suo contenuto, tanto da equipararsi alla firma tradizionale⁷.

In particolare, come ha giustamente riferito M. Scialdone⁸, <<il concetto di firma elettronica è tuttavia molto ampio e include tutte le tecniche utilizzate per identificare una persona in ambiente elettronico e può essere espresso nei seguenti termini: la firma elettronica consiste in qualsiasi marcatura elettronica che indichi l'identità di un soggetto da considerarsi firmatario del documento. A titolo meramente esemplificativo possono essere definite come firme elettroniche l'abbinamento “user id- password”, tecnologie biometriche, quali la scannerizzazione della retina, tecnologie crittografiche e qualunque altro strumento in grado di adempiere alla funzione sopra descritta. La differenza fondamentale che intercorre tra le diverse tipologie di firma elettronica è rappresentata, oltre che dalla tecnologia utilizzata, anche dalla loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi richiesti per garantire la manifestazione di volontà da parte del soggetto firmatario, nonché l'integrità e l'immodificabilità del documento così firmato. Allo stato attuale, la soluzione tecnica in grado di garantire maggiormente la presenza degli elementi da ultimo richiamati è rappresentata dalla firma digitale⁹>>.

Ovviamente le difficoltà maggiori che si sono riscontrate nell'adeguamento e sviluppo della normativa sul documento informatico e sulla firma elettronica sono state determinate dalla assoluta diversità ontologica sussistente con il documento cartaceo alle cui certezze dogmatiche si è cercato di riportare il concetto di documento informatico. Eppure viene sempre più avvertito da più parti come il documento informatico debba piano piano costituire un *genus* proprio, autonomo e slegato dalle “certezze” tradizionali della sottoscrizione, per farlo progredire verso concetti nuovi, che prescindano dalla fisicità dell'appartenenza del documento al suo autore (tipica della sottoscrizione cartacea) sino a seguire gli orizzonti giuridici di una appartenenza del documento informatico legata alla disponibilità dello strumento telematico e al potere di controllo sullo stesso¹⁰. Inoltre, è utile

⁶ L. Ponti e P. Panella, “*Il Contratto telematico: firma digitale*”, in “I nuovi contratti nella prassi civile e commerciale”, vol. IX, a cura di P. Cendon, Torino, 2004, pag. 238.

⁷ In proposito, nella più ampia categoria delle firme elettroniche, si distinguono le **firme elettroniche <<sicure>> o <<avanzate>>**, in quanto posseggono requisiti e funzionalità che offrono garanzie tali da poterle paragonare, agli effetti legali, alle sottoscrizioni tradizionali cartacee. La Direttiva CE definisce per <<firma elettronica avanzata>>, *una firma elettronica che soddisfi i seguenti requisiti: a) essere connessa in maniera unica al firmatario; b) essere idonea ad identificare il firmatario; c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati (art. 2, comma 2). Ai fini dell'attribuzione degli effetti giuridici (art. 5), viene, poi, ulteriormente distinta la <<firma elettronica sicura>>, che è apposta con un dispositivo che soddisfa i requisiti posti dall'Allegato III della direttiva (art. 1, n. 6). Queste definizioni adottano un approccio aperto, che non presuppone il necessario impiego di una tecnologia determinata, lasciando il campo aperto a tutti quei sistemi che realizzano, comunque, i requisiti e le funzioni indicati (così R. Zagami, “*Firma digitale e sicurezza giuridica*”, Cedam, Padova, 2000, pag. 33).*

⁸ Nel volume “Guida al Codice dell'Amministrazione Digitale”, a cura di A. Lisi e L. Giacomuzzi, Halley Editrice, 2006.

⁹ Come vedremo meglio in seguito la firma digitale è un particolare tipo di sottoscrizione elettronica basata su un sistema di chiavi asimmetriche a coppia, pubblica e 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.

¹⁰ Già nel 1982, una autorevole dottrina aveva correttamente inquadrato il nuovo fenomeno in termini giuridici: “l'elaborazione del valore giuridico del messaggio trasmesso per telex è agli inizi. Il telex memorizza un messaggio, senza identificare il mittente. Il messaggio però identifica l'apparecchio trasmittente. In altre parole: il telex non dice con sicurezza chi ha inviato il messaggio, ma dice chi è l'utente (più esattamente: chi ha titolo per l'uso) e, quindi, chi è responsabile dell'apparecchio trasmittente [...]. La dichiarazione per telex individua il soggetto di un potere giuridico a cui si accompagna di norma un potere di fatto” (così R. Sacco, *Trattato di Diritto Privato*, diretto da Pietro Rescigno, Vol. II Obbligazioni e Contratti, UTET, 1982, 242). E ancora la stessa dottrina così si esprime più recentemente: “in tema di contratto informatico tornano a presentarsi i problemi che abbiamo incontrato a proposito del telegrafo e del

sottolineare come strettamente connesso al concetto di documento informatico e di firma elettronica ci dovrà essere sempre il profilo della *e-security*.

Nella vigenza del D. Lgs. n. 10/2002 poteva, comunque, essere fornita una risposta positiva al quesito fondamentale che ci siamo posti e, cioè, se un documento elettronico in qualche modo appartenente ad un soggetto tramite un sistema di autenticazione informatica (come una ID e una PW di accesso ad un sistema protetto finalizzato a gestire transazioni commerciali) potesse soddisfare il requisito della forma scritta: si trovava, infatti, conforto nell'articolo 10, 2° comma, del DPR 445/2000 (come modificato dal D.Lgs. n. 10 del 2002 di recepimento della direttiva sulle firme elettroniche e, quindi, del principio della neutralità tecnologica in ambito comunitario). Tale articolo, disciplinando la forma e l'efficacia del documento informatico, prevedeva che:

1) *Il documento informatico ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate.*

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 (libri obbligatori e altre scritture contabili) e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.*

3) *Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma sono basati su di un certificato qualificato, generato mediante un dispositivo per la creazione di una firma sicura, facendo piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.*

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.**

Infatti - considerato che secondo il D.Lgs. n.10/2002, art. 2, la firma elettronica altro non era che *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica* e posto che per "autenticazione informatica" doveva intendersi *l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità* (art. 4, comma 3 lettera c), del D.Lgs. 196/2003) – allora sembrava naturale, secondo l'attenta lettura di tali disposizioni, considerare documento informatico "scritto" (liberamente valutabile dal giudice dal punto di vista probatorio) qualsiasi manifestazione di volontà telematica che fosse in qualche modo attribuibile al suo autore attraverso una qualsivoglia forma di "autenticazione informatica"¹¹.

telex. (...) Chi mette in funzione un computer deve poi far fronte alle conseguenze - in particolare agli affidamenti - che scatena. Deve far fronte ai messaggi che inoltra; deve far fronte ai messaggi che i suoi incaricati (fedeli o infedeli) inoltrano" (R. Sacco, Trattato di Diritto Privato, diretto da P. Rescigno, 2004, 83).

¹¹ Questa interpretazione è stata confermata da numerosi decreti ingiuntivi, emessi da diversi giudici, sulla base della presentazione di una semplice e-mail di cui si è accennato in precedenti note. Il tutto sulla considerazione che <<il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. La firma elettronica, infatti, è l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica. Per questo l'e-mail può essere considerato un documento informatico provvisto di firma elettronica, nella quale la coppia di dati "indirizzo mittente – headers" associati logicamente alla coppia di dati "username e password" soddisfa il requisito della forma scritta>>, come disponeva l' art. 10, comma 2, del D.P.R. n. 445/2000. In linea con questa interpretazione, molti scritti pubblicati sul web (tutti rintracciabili sul sito www.scint.it): "Il valore del documento elettronico nell'aula di un Tribunale! Alcune riflessioni a proposito delle ultime pronunce giurisprudenziali sul valore dell'e-mail" di A. Lisi; "Dal CNIPA un po' di chiarezza su firme elettroniche "leggere" e "pesanti": User Id e Pw possono essere considerati firma elettronica!" di A. Lisi; "Anche per il CNIPA l'e-mail equivale a "forma scritta"!" di A. Lisi; "Il documento informatico "scritto" (ma non sottoscritto) nel commercio elettronico internazionale: le ultime conferme in Italia e in Europa" di A. Lisi; "Quando la posta elettronica ha forza di documento scritto" di R. Manno; "Firme elettroniche e crisi del principio di unitarietà della sottoscrizione" di F. Sarzana di Sant'Ippolito; "Provider ed e-mail probatorie" di S. Camerini; "L'e-mail è forma

Il combinato disposto di tali prescrizioni portava a dire, per quanto più da vicino ci interessa, che **il documento informatico privo di qualsiasi forma di firma era, quindi, equiparabile ad una mera riproduzione meccanica** i cui effetti sono anche oggi quelli previsti dall'art. 2712 cod. civ.; **mentre il documento informatico provvisto della firma elettronica anche "leggera" soddisfaceva il requisito legale della forma scritta.** È facile arguire a questo punto come la prassi negoziale on line di cui si discute si sarebbe potuta tranquillamente ritenere legittima, solo ove essa si potesse in qualche modo ricondurre on line al documento elettronico provvisto di una qualsivoglia firma elettronica. Ma non sempre è così nei siti web di commercio elettronico: perché qualora non sussista un metodo per assicurare una biunivoca corrispondenza tra gestore del sito, da un lato, e utente del sito stesso, dall'altro lato, allora non si è in presenza di alcuna firma elettronica. Manca, cioè, quel sistema di autenticazione informatica che era (ed è anche oggi) richiesto dalla legge per aversi un documento informatico provvisto di firma elettronica semplice ed idoneo, in quanto tale, a soddisfare il requisito legale della forma scritta (art. 10, II, DPR 445/00).

Un sistema di autenticazione si può ottenere, invece, nel momento in cui l'utente registrato acceda all'area riservata utilizzando i propri codici personali di accesso (ID più PW) previamente forniti all'utente stesso al momento della richiesta di registrazione.

È, quindi, nel momento in cui l'utente registrato accede per la prima volta alla "*personal zone*" che deve richiedersi il consenso al trattamento dei dati personali; consenso che potrà così ritenersi legalmente anche documentato per iscritto e dirsi, così, validamente prestato. E nella stessa area riservata è opportuno inserire chiare informative per il consumatore e condizioni contrattuali da far sottoscrivere con il "point&click"¹².

Si ricorda, inoltre, che rimane sempre necessario confermare via e-mail le condizioni generali di contratto fatte sottoscrivere al proprio utente ai sensi del secondo comma dell'art. 13 del D. Lgs. 70/2003 (già in precedenza citato nel presente capitolo).¹³

Quella fornita è comunque solo una possibile lettura delle norme in vigore prima dell'avvento del Codice dell'Amministrazione Digitale: interpretazione che mirava ad assicurare un minimo di legittimità giuridica alle prassi del commercio elettronico e sembrava trovare qualche

scritta?" di A. Lisi; "Email e requisito di forma scritta" di M. Cuniberti; "L'e-mail dal commercio elettronico alle aule di giustizia" di A. Lisi; "Quando la «chiocciolina» entrò nelle aule di giustizia brevi considerazioni a margine di due recenti decreti ingiuntivi emessi in forza dell'e-mail" di G. Cassano e I.P. Cimino; "Rilevanza giuridica del documento informatico. Nuovi sviluppi e nuova giurisprudenza: il "famigerato" d.i. del Tribunale di Cuneo" di G. Lazari.

¹² Appare, invece, facilmente superabile l'obiezione secondo cui la soluzione proposta porrebbe comunque il problema del consenso al trattamento dei propri dati personali (almeno l'indirizzo e-mail) per farsi inviare i codici di accesso all'area riservata. Invero, sul punto è sufficiente considerare che l'invio di tali codici rappresenti null'altro che l'adempimento, prima della conclusione del contratto, ad una specifica richiesta dell'interessato per il quale – ai sensi della lett. b) dell'art. 24 – non è necessario il previo consenso.

¹³ Una importante sentenza del Giudice di Pace di Partanna alla fine del 2001 aveva sposato la teoria del "doppio click" ai fini dell'accettazione delle clausole vessatorie. Si tratta della nota **sentenza del Giudice di Pace di Partanna n. 15/2002**. Cassano e Cimino (in *Contratto via internet e tutela della parte debole: commento a GdP Partanna 15/02*, in *I Contratti*, Ipsoa, 2002), a commento della sentenza, precisano: "La doppia approvazione, nella contrattazione on line, si concretizzerebbe o nell'utilizzo della firma digitale, oppure nella effettuazione - da parte dell'aderente alla proposta contrattuale predisposta sul sito web - di un doppio click di accettazione: un primo sul «tasto» relativo all'adesione all'intero regolamento contrattuale, ed un secondo sul «tasto» relativo all'approvazione specifica delle clausole vessatorie ivi inserite". Tale sentenza, pur lungimirante e rivoluzionaria, era ancora piuttosto ingenua e criticabile nel momento in cui non aveva approfondito l'argomento a sostegno della tesi esposta dal punto di vista strettamente giuridico-informatico (sia dal punto di vista della presenza di una firma elettronica nel sito web di e-commerce, sia dal punto di vista della stessa sicurezza informatica della transazione on line).

accreditamento in recenti precedenti giurisprudenziali¹⁴ e numerosi avalli nella dottrina più attenta alle esigenze dell'impresa.

In verità, la problematica è molto complessa e non poteva essere facilmente risolta a causa della presenza di una normativa, quella italiana, che soddisfaceva le necessità formali della P.A., ma non quelle più concrete (e dettate dalla convenienza dello strumento) degli imprenditori: essa riconosceva piena validità formale e probatoria ai soli documenti provvisti di firma digitale (come vedremo, una particolare forma di firma elettronica sicura e basata su certificati qualificati) e soprattutto si trattava di una normativa che era stata oggetto di continui rimaneggiamenti e evoluzioni (o involuzioni!).

Un sostegno alla validità delle transazioni commerciali telematiche lo si è sempre trovato, invece, a livello internazionale, dove normative, prassi e leggi modello (si fa riferimento ai Principi Unidroit, alla Convenzione di Vienna sulla vendita internazionale, alla Legge Modello Uncitral sul commercio elettronico) tendono a garantire elasticità alle contrattazioni *on line* cercando di favorirne lo sviluppo.

A livello internazionale e comunitario un telefax, un telex, un telegramma e una e.mail soddisfano da tempo il requisito della "forma scritta" e, quindi, un messaggio può essere considerato "*written*" qualora l'informazione contenuta ha i requisiti di *identificabilità* dell'utente che l'ha generata e di *conservazione durevole* del suo contenuto. *La firma* in senso stretto non è ritenuta più indispensabile se il mittente ha applicato una qualche procedura di autenticazione (anche se la stessa non soddisfa i requisiti di assoluta sicurezza).

Il Codice dell'Amministrazione Digitale (D. Lgs. 82/2005), ha cercato proprio di garantire maggiore certezza nell'interpretazione giuridica di queste nuove manifestazioni di volontà e - seppure nella sua prima stesura entrata in vigore nel 1° gennaio del 2006, ha rischiato di far fare un ulteriore passo indietro alla normativa (ricevendo sonore critiche dal Consiglio di Stato¹⁵) - successivamente il legislatore nelle nuove norme modificative del decreto (D. Lgs. 156/2006) ha quanto meno cercato di fare ordine e di dare attuazione ai principi espressi nella legge delega¹⁶.

¹⁴ Tra i più recenti interventi giurisprudenziali si ricorda, anche, la **recente ordinanza del Tribunale di Bari del 2 giugno 2005** – Relatore Dr. F. Cassano – nella quale si afferma : <<allo stato, ed in generale, l'e-mail deve essere considerata un documento informatico che soddisfa il requisito della "forma scritta" ai sensi dell'art. 6 d.lgs. n. 10/2002 (cfr. Trib. Cuneo, 15 dicembre 2003, n. 848, in www.dirittoegiustizia.it; Trib. Bari, 19 dicembre 2003-20 gennaio 2004, n. 89, in www.dirittoegiustizia.it). Ciò in quanto si tratta di documento provvisto di firma elettronica leggera, o "debole", cioè di un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 2, lett. a, d.lgs. 10/2002)>> (pubblicata alla pagina http://www.scint.it/news_new.php?id=664).

¹⁵ <<In materia di rilevanza e valore del documento informatico, minori problemi crea il vigente articolo 10 del d.P.R. n. 445 del 2000 - che per il documento informatico in sé, a prescindere dalla sottoscrizione, rinvia all'articolo 2712 c.c. e prevede (comma 2) che il documento informatico sottoscritto con firma elettronica soddisfa il requisito della forma scritta, dandosi così carico di attribuire un valore a qualsiasi documento informatico, a prescindere dalla forza della firma - rispetto agli articoli 17 e 18 dell'emanando Codice dell'amministrazione digitale, che non stabiliscono come debba essere considerato l'atto con firma elettronica debole non disconosciuta a norma dell'articolo 215 c.p.c.>> (così Consiglio di Stato, nel parere 11995/05).

¹⁶ I delicati compiti, i principi e i criteri che il legislatore avrebbe dovuto perseguire nell'emanazione del nuovo Codice della amministrazione digitale sono ben indicati nella **legge delega 229/2003**. In particolare, la legge delega affidava al Governo il compito di:

- a) graduare la rilevanza giuridica e l'efficacia probatoria dei diversi tipi di firma elettronica, in relazione al tipo di utilizzo e al grado di sicurezza della firma;
- b) rivedere la disciplina vigente al fine di garantire la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici e di assicurare ai cittadini e alle imprese l'accesso a tali servizi secondo il criterio della massima semplificazione degli strumenti e delle procedure necessari e nel rispetto dei principi di eguaglianza, non discriminazione e della normativa sulla riservatezza dei dati personali;
- c) prevedere la possibilità di attribuire al dato e al documento informatico, contenuto nei sistemi informativi pubblici, i caratteri della primarietà e originalità, in sostituzione o in aggiunta a dati e documenti non informatici,

3. Le firme elettroniche nel Codice dell'Amministrazione Digitale (CAD)

Il Decreto Legislativo 82/2005 (come modificato dal D.Lgs 156/2006) ha ridotto a due le tipologie di firma elettronica, in stretta aderenza alla normativa comunitaria e come suggerito dallo stesso Consiglio di Stato: la firma elettronica e la firma elettronica qualificata (la firma digitale viene, invece, identificata come una particolare tipologia di firma elettronica qualificata)¹⁷.

Il Codice, quindi, considera oggi nel suo **articolo 1** dedicato alle definizioni:

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

A regolamentare oggi la materia del valore formale e probatorio del documento informatico sono gli **articoli 20 e 21 del CAD**.

Considerata la loro importanza, si ritiene utile riportare qui di seguito nella loro completezza i due articoli citati:

Art. 20 Documento informatico

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

3. Le regole tecniche per la formazione, trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione

nonché obbligare le amministrazioni che li detengono ad adottare misure organizzative e tecniche volte ad assicurare l'esattezza, la sicurezza e la qualità del relativo contenuto informativo;

d) realizzare il coordinamento formale del testo delle disposizioni vigenti, apportando, nei limiti di detto coordinamento, le modifiche necessarie per garantire la coerenza logica e sistematica della normativa anche al fine di adeguare o semplificare il linguaggio normativo;

e) adeguare la normativa alle disposizioni comunitarie.

¹⁷ <<Anche in considerazione della Direttiva comunitaria n. 1999/93/CE, che ha introdotto un quadro comunitario per le firme elettroniche, i tipi di firma sono solo due, la firma elettronica pura e semplice e quella qualificata, di cui la firma digitale è un tipo>> (così Consiglio di Stato, nel parere 11995/05).

del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Art. 21

Valore probatorio del documento informatico sottoscritto

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

I due articoli, pur se ancora criticabili sotto certi punti di vista (ma ai nostri fini è inutile dilungarci su questo), confermano l'interpretazione fornita, nella vigenza del D. Lgs. 10/2002, da quella parte della dottrina e giurisprudenza che considerava utile garantire alle prassi di e-commerce e alle stesse e-mail una qualche validità formale e probatoria (considerandoli documenti informatici scritti).

Il legislatore, quanto meno oggi e nel futuro più immediato (considerate le continue modifiche normative che hanno caratterizzato la materia nell'ultimo periodo è giusto essere cauti!), ritiene essere sufficiente la firma elettronica semplice (e, quindi, anche una semplice User Id e Password) perché al documento informatico sia riconosciuta una validità giuridica.

Con il Codice dell'Amministrazione Digitale, e in particolare con le modifiche contenute nel D. Lgs. 156/2003, il legislatore ha così operato una corretta separazione tra l'ambito formale e l'ambito probatorio: la "forma scritta" verrà addirittura garantita dal documento informatico in quanto tale, purché esso abbia un minimo di affidabilità tecnica. In questo modo, il legislatore ha voluto in qualche modo legare la normativa generale contenuta nel Codice con quella speciale dedicata alla formazione del documento informatico (ad esempio, il D.P.C.M. 23 gennaio 2003) e alla conservazione ottica sostitutiva dei documenti (si fa riferimento alla Deliberazione Cnipa n. 11 del 19 febbraio 2004 e al Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004). In queste ultime normative, infatti, il concetto di documento informatico valido e rilevante è accostato alle sue caratteristiche intrinseche di immodificabilità e staticità¹⁸, anche a prescindere dalla presenza di una sottoscrizione digitale nello stesso.

I concetti di sottoscrizione e firma elettronica, dal punto di vista sistematico, riguarderebbero più propriamente l'ambito probatorio, relativo alla provenienza del documento informatico (che

¹⁸ Garantite, ad esempio, dalla mancanza nel documento di codici eseguibili e macroistruzioni.

rimarrebbe pur sempre, nella sua essenza e in presenza di determinate caratteristiche di sicurezza, "forma scritta").

Questa evoluzione del concetto della "forma scritta" - legata alla natura del documento informatico e ad una certamente problematica valutazione giudiziale delle sue caratteristiche tecniche - opera, in maniera opportuna, una cesura con il passato: non si sarebbe più in presenza di una *condicio sine qua non* tra rigida appartenenza del documento informatico a qualcuno attraverso i sistemi della firma digitale e validità formale di quella dichiarazione negoziale. Ovviamente, se pur ci sentiamo di approvare questa evoluzione teorica, occorrerà con il tempo approfondirla e svilupparla¹⁹.

Certamente possiamo riferire che oggi le procedure di e-commerce sono in qualche modo garantite da questa normativa, nel momento in cui associano le procedure di autenticazione informatica a procedure di sicurezza (anche affidate a processi di conservazione sostitutiva dei *log file* generati dalle transazioni sviluppate nelle loro aree riservate, in linea con le regole tecniche attualmente in vigore)²⁰. Questo tipo di evoluzione normativa consentirà un ulteriore sviluppo di sistemi pubblici e privati di e-commerce e e-procurement più attenti alle esigenze di sicurezza (si pensi alle esperienze nazionali e internazionali di transazioni o di scambio di dati "blindati" tra server). Così come è indubbio che questo processo normativo consentirà di spostare l'attenzione da forme di "certificazione pubblica" legata al solo strumento della firma digitale (ancora purtroppo inutilizzata nel settore privato di scambio commerciale) a forme di certificazione della transazione commerciale on line affidate a terze parti fidate (anche private)²¹. Occorre sottolineare, cioè, che se

¹⁹ In verità, il legislatore sembrerebbe aver accolto favorevolmente le sollecitazioni contenute in un saggio pubblicato pochi mesi prima dell'entrata in vigore del decreto correttivo, nel quale si evidenziava come: «<nella ricostruzione della categoria del *genus* della forma scritta, non si potrà non attribuire alle varie *species* una valenza giuridica differenziata: per esempio, il mero riconoscimento alla e-mail del rango di atto avente forma scritta non implica automaticamente anche la facoltà giuridica di compiere, attraverso tale strumento, degli atti traslativi della proprietà di beni immobili, in quanto l'art. 1350 c.c. riserva espressamente tale possibilità solo all'atto pubblico e alla scrittura privata. D'altra parte è necessario concentrare l'attenzione e, quindi, attribuire maggior rilevanza alla dichiarazione contenuta nel documento e all'idoneità del mezzo concretamente adottato a raggiungere lo scopo perseguito dalla norma, che prescrive una determinata forma» (così Lisi - Lazari in "Analisi del Parere del Consiglio di Stato 11995/05 alla luce dell'evoluzione del concetto di documento informatico: verso il necessario superamento della sottoscrizione nella scrittura telematica tra privati", in *Giurisprudenza Italiana*, Utet, 2005, pp. 1164-1168).

²⁰ Attraverso l'utilizzo di tecniche di sicurezza informatica e di conservazione sostitutiva dei documenti è superabile anche la critica relativa all'acquisizione probatoria di documenti informatici pubblicati on line contenuta nella recente sentenza della Corte di Cassazione (**Cass. Sez. Lavoro Sent. 02912/04**), secondo la quale "le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione e, a prescindere dalla ritualità della produzione, va esclusa la qualità di documento in una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento".

²¹ Questa evoluzione normativa sembra trovare riscontro in due altre norme del CAD pensate per i siti delle P.A., gli artt. 64 e 65, i quali possono essere considerati degli "apripista" anche per il settore privato, purché sia chiaro che non si possa prescindere da una seria valutazione delle procedure di sicurezza informatica e conservazione dei log file nella realizzazione di tali siti web. Si ritiene utile riportare qui di seguito i due articoli citati:

Art. 64

Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.
2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni [...].

Art. 65

Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:
 - a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
 - b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

anche la normativa italiana (ed europea) consenta oggi di attribuire un qualche valore formale ad uno scambio di semplici e-mail o ad una contrattazione telematica preceduta da un processo di autenticazione dell'utente, è sempre necessario avvalersi di strumenti di negoziazione che assicurino uno scambio di dati informatici sicuri e protetti, affidandosi sempre e comunque a forme di certificazione²².

4. Cenni alla firma digitale e alla posta elettronica certificata

Come già accennato in precedenza, da un punto di vista più propriamente tecnico, **la firma digitale** (l'unica tra le firme elettroniche qualificate disciplinate nella Direttiva 1999/93/CE a essere già stata implementata nel nostro Paese) è un insieme di *bit* logicamente associati a un documento informatico e generati mediante l'impiego di un apposito dispositivo sicuro di firma. I complessi algoritmi di cifratura su cui poggia tale "meccanismo" garantiscono il rispetto di precisi requisiti di sicurezza. A voler scendere ulteriormente nel dettaglio, la firma digitale si basa sulla tecnologia della crittografia, la scienza che studia le tecniche che consentono di trasformare un messaggio per così dire "in chiaro", in uno leggibile, soltanto per coloro che possano disporre della chiave di decifrazione; nello specifico si tratta di un sistema di cifratura asimmetrico (o a chiave pubblica) dei dati informatici. Cifrare, infatti, deriva dal verbo greco "κρύπτω"²³, cioè "io nascondo". Criptare pertanto significa trasformare i dati in una forma incomprensibile e illeggibile da parte di chi non possieda la chiave per effettuare l'operazione inversa di decifrazione.

Un sistema di cifratura asimmetrico, quale quello adottato dal legislatore italiano, funziona con coppie di chiavi tra loro diverse e matematicamente collegate: una chiave privata e una chiave pubblica; ciò che una chiave cifra, l'altra decifra.

Le proprietà fondamentali di una tale sistema sono, quindi:

- ✓ non si può decifrare il testo con la stessa chiave usata per cifrarlo;
- ✓ le due chiavi sono generate con la stessa procedura e correlate univocamente;
- ✓ conoscendo una delle due chiavi non c'è nessun modo di ricostruire l'altra.

La chiave privata, ovviamente, è destinata a rimanere segreta mentre la chiave pubblica ad essere divulgata. In tutto il processo della firma digitale è necessario l'intervento di una "**terza parte fidata**" (*trusted third part*), generalmente nota come **Certification Authority** (nel nostro ordinamento "**il certificatore**"), alla quale è affidata anche la gestione dei registri contenenti le chiavi pubbliche.

L'uso di sofisticati algoritmi matematici, di cui si serve la firma digitale, consente pertanto:

- la **segretezza** del contenuto dell'informazione;
- l'**autenticità**, individuando univocamente la fonte del messaggio;
- l'**integrità** del documento, verificando che il messaggio non abbia subito alterazioni;

c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'articolo 64, comma 3.

2. Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante la firma digitale.

²² L'**utilizzo di e-mail certificate** (anche attraverso sistemi internazionalmente riconosciuti come il protocollo S-MIME) nello scambio di dati commerciali **o comunque di processi di negoziazione affidati a certificazione SSL, assicura alla contrattazione una maggiore sicurezza e un rispetto della normativa** (anche di quella dedicata alla protezione dei dati personali, come recentemente affermato da L. de Grazia nel suo articolo *Pagamenti on line e sicurezza: la posizione giuridica degli istituti bancari* ospitato sulla Newsletter di GlobalTrust del 26 agosto 2005 n. 6).

²³ Pron. "kripto".

- il **non ripudio**, assicurando che l'autore del messaggio non possa negare di aver formato il documento stesso.

L'enorme forza di cui è dotata tale tipologia di sottoscrizione consente al documento informatico dotato di firma digitale una piena parificazione normativa con il documento cartaceo sottoscritto (anzi il Codice della Amministrazione Digitale fa di più, operando una presunzione di riconducibilità della firma digitale al suo titolare).

A voler essere sinceri, la firma digitale, pur se il suo impiego è (giustamente) obbligatorio in alcune specifiche ipotesi previste dalla legge²⁴, è ancora troppo poco (o forse per nulla) diffusa nel settore della contrattazione privata per poterla seriamente prendere in seria considerazione nella nostra analisi.

Alcuni cenni merita anche la **posta elettronica certificata**. Essa è prevista e regolamentata dal DPR dell'11 febbraio 2005, n. 68 e consiste in un sistema di posta elettronica nel quale è fornita al mittente la certificazione elettronica attestante l'invio e la consegna di documenti informatici.

"Certificare" la trasmissione del documento informatico significa fornire al mittente, dal proprio gestore di posta, una ricevuta certificata attestante l'avvenuta spedizione del messaggio (e contenente anche l'eventuale allegata documentazione). Allo stesso modo, quando il messaggio perviene al destinatario, il gestore di posta elettronica certificata del destinatario invia al mittente la ricevuta di avvenuta (o mancata) consegna (con l'indicazione temporale).

Nel caso in cui il mittente dovesse smarrire le ricevute, la traccia informatica di tutte le operazioni svolte, deve essere conservata a cura dei gestori per un periodo di 30 mesi. Potranno scambiarsi le e-mail certificate sia i privati, sia le PA.²⁵

Potranno svolgere servizi di PEC solo i gestori iscritti in apposito elenco tenuto dal Cnipa (che verificherà i requisiti soggettivi ed oggettivi inerenti ad esempio alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo) e, per iscriversi nell'elenco, essi dovranno possedere un capitale sociale minimo non inferiore a un milione di euro e presentare una polizza assicurativa contro i rischi derivanti dall'attività di gestore²⁶.

²⁴ Si pensi, ad esempio., alla notificazione al Garante per il trattamento dei dati personali prevista dall'art. 37 del Codice della privacy, o alle comunicazioni dei registri camerali, o alle ipotesi di materializzazione delle scritture contabili e dei documenti rilevanti fiscalmente (D.M.E.F. 23 gennaio 2004 e Deliberazione CNIPA n. 11/2004), o ancora alla fatturazione elettronica (D. Lgs. 52/2004).

²⁵ Le imprese, nei rapporti intercorrenti, potranno dichiarare l'esplicita volontà di accettare l'invio di PEC mediante indicazione nell'atto di iscrizione delle imprese.

²⁶ In proposito, non si può non essere d'accordo con quanto riferito da F. Bertoni (nel volume "Guida al Codice della Amministrazione Digitale", a cura di A. Lisi e L. Giacomuzzi, Halley Editrice, 2006) e che qui si riporta testualmente: << Alcune considerazioni meno entusiastiche meritano, comunque, di essere espresse soprattutto in riferimento all'utilità ed ai benefici che questo strumento porterà ai futuri rapporti tra P.A., imprese e privati cittadini. L'utilità del PEC, infatti, è legata alla sua continua diffusione tra gli operatori commerciali e tra i cittadini in genere; al riguardo, la pubblica amministrazione centrale dovrà avvalersi [Ndr. meglio dire avrebbe dovuto avvalersi!] di tale strumento come mezzo di comunicazione interno entro otto mesi dall'entrata in vigore del codice, utilizzando quest'ultima anche per le comunicazioni tra amministrazione e pubblici dipendenti, garantendo il rispetto dei dati personali e fornendo l'informativa circa la riservatezza degli strumenti utilizzati (secondo l'art. 47 III comma lett. a e b). Un suo sviluppo a "macchia di leopardo", pertanto, non potrà certamente contribuire allo sviluppo di tale mezzo di comunicazione, se si considera, inoltre, che il livello alfabetizzazione informatica nelle P.A. e nell'utenza in generale non raggiunge ancora un grado soddisfacente. Al riguardo occorre tener presente che, talvolta, anche il legislatore ci mette del suo nel frenare lo sviluppo di questo sistema: si fa riferimento all'art. 14, comma 3, del suindicato DPR n. 68/2005 laddove si afferma che "i richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro". Emerge chiaramente una ingiustificata discriminazione verso i gestori che non possiedono un tale capitale sociale, venendo così automaticamente esclusi. A parere di scrive, infatti, in questo modo si perde di vista quello che deve essere l'obiettivo primario e, cioè, favorire lo sviluppo delle nuove tecnologie ed incentivare e velocizzare le informazioni telematiche>>.

Anche per quanto riguarda la PEC si può ripetere il discorso fatto per la firma digitale: il suo utilizzo nei rapporti privati è ancora limitatissimo.

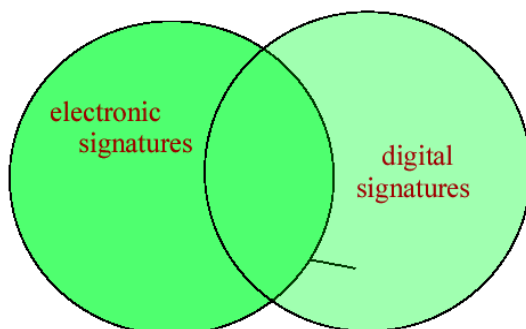
Le ragioni di questo scarso utilizzo sono molteplici; certamente questi strumenti non sono stati anticipati da una adeguata campagna di sensibilizzazione e alfabetizzazione informatica e sono avvertiti dal “popolo del web” come delle imposizioni piuttosto che delle adeguate misure tecnologiche per garantire una maggiore sicurezza (e validità) alle contrattazioni on line. Inoltre, occorre riferire che l’interoperabilità e la “usability” di tali strumenti a volte lascia un po’ a desiderare e, soprattutto per quanto riguarda la PEC, essa – così come configurata dalla normativa italiana – è inutilizzabile a livello internazionale²⁷. Infine, non possiamo dimenticare che è operazione difficile, complessa e, forse, inutile provare *ex lege* ad anticipare le prassi commerciali invece di osservarle ed eventualmente regolamentarle. Sta di fatto che oggi il WWW va per conto suo, infischandosene di questi strumenti e autoregolamentandosi con forme libere di certificazione, slegate dalla “*longa manu*” statale²⁸.

²⁷ La posta elettronica certificata contenuta nella normativa italiana prevede un processo di sottoscrizione della busta affidato ai provider accreditati a fornire questo tipo di servizio e – per sprigionare i suoi “effetti legali” – rimane necessario l’accordo tra mittente e destinatario. Per le sue caratteristiche di “unicità” nel panorama internazionale e di “mancanza di interoperabilità” con altri sistemi di trasmissione dei messaggi, **la normativa italiana in materia di PEC risulta essere, a parere di chi scrive, a rischio di disapplicazione comunitaria perché in contrasto con i principi di neutralità e unitarietà espressi dalla direttiva 1999/93/CE.**

²⁸ Si fa riferimento, ad esempio, ad ipotesi di posta elettronica affidate a terze parti fidate o comunque di ISP affidabili che possano offrire servizi potenzialmente sicuri (e disponibili contrattualmente anche a fornire davanti ad un Giudice la “prova informatica” delle transazioni commerciali intervenute attraverso i loro servizi). Si guardi, ad esempio, il servizio di *Mail Service* (o ancora di *Global Service*) offerto dal Gruppo CM Trading (si veda http://www.gruppocmtrading.it/servizi.asp?l_page=Servizi&l_class=offertaback&l_menu=SE). O ancora molto interessante risulta essere l’ipotesi di certificazione di e-mail a cura di un gruppo di notai europei: “Le transazioni e-mail possono essere autenticate dai notai: un gruppo di notai europei sceglie di non restare escluso da un mercato in evoluzione e offre un servizio on-demand” disponibile alla pagina http://www.scint.it/news_new.php?id=804. Per poi arrivare a forme di certificazione sicure e internazionalmente garantite come i servizi offerti da vere e proprie società di certificazione di natura privata (come i servizi di posta elettronica certificata e di certificazione del sito offerti, ad esempio, da GlobalTrust – www.globaltrust.it). Naturalmente per offrire certi servizi ci vuole competenza tecnica e capacità di valutazione giuridica ed è indispensabile costituire *team* di esperti per sviluppare servizi veramente utili, innovativi e in linea con il dettato normativo.

SCHEMI DI SINTESI

Fig. 1– Firme elettroniche e Digitali in Europa:

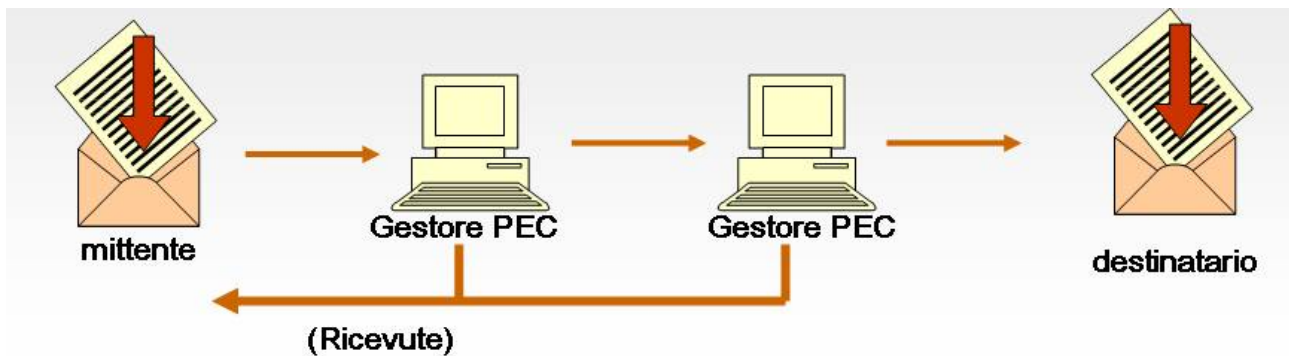


Fonte relazione Prof. Jos Dumortier – acquisibile alla pagina <http://convegno.giuristitelematici.it/relatori.htm>

Fig. 2 – Validità formale e probatoria del Documento informatico, delle Firme elettroniche e Digitali nel Codice dell'Amministrazione Digitale:

<p>▪ TABELLA RIEPILOGATIVA</p>		
<p>○ ○ DOCUMENTO INFORMATICO</p>		
<p>Documento informatico non sottoscritto</p>	<p>È valido e rilevante a tutti gli effetti di legge, ai sensi delle disposizioni del Codice. La sua idoneità a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche di qualità, sicurezza, integrità e immodificabilità.</p>	<p>Ha l'efficacia probatoria di cui all'art. 2712 c.c.</p>
<p>Documento informatico sottoscritto con firma elettronica semplice</p>	<p>La sua idoneità a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche di qualità, sicurezza, integrità e immodificabilità.</p>	<p>Sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza, integrità e immodificabilità.</p>
<p>Documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata</p>	<p>Soddisfa il requisito legale della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del Codice Civile</p>	<p>Ha l'efficacia probatoria di cui all'art. 2702 c.c., ma l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data da quest'ultimo prova contraria</p>

Fig. 3 – Posta elettronica certificata secondo il DPR dell'11 febbraio 2005, n. 68



5. La “certificazione” del sito web e dei processi di negoziazione

<<Le caratteristiche di a-nazionalità tipiche di Internet spesso causano nell’utente un profondo senso di “disagio” e di “insicurezza”, poiché, pur essendone attratto, egli teme il “lato oscuro” del Web, consapevole del fatto che quando è l’immaterialità a caratterizzare i rapporti, il bisogno di certezze e affidabilità aumenta vertiginosamente. Così anche le attività di commercio elettronico e di scambio di dati, per poter diventare una serena abitudine, debbono necessariamente fondarsi su un insieme di tecniche idonee a rispondere alle esigenze di sicurezza che gli “users” avvertono, mentre navigano>>, così F. Bertoni e G. Garrisi²⁹

Strumenti quali la certificazione del sito web e degli scambi di dati, nonché idonee *policies* di sicurezza informatica abbinate a una corretta conservazione dei dati, possono, infatti, rendere il mercato virtuale addirittura più sicuro di quello reale.

Accennavamo innanzitutto alla “**certificazione**” del sito web. Diffusa a livello internazionale, in Europa e ormai anche in Italia, la certificazione del sito è una sorta di “bollino di qualità” (detto anche “seal of approval” o “trustmark”), a cui un sito di e-commerce decide liberamente di sottoporsi (attraverso la sottoscrizione di un contratto) per conquistare la fiducia del *cyberconsumatore* e più in generale per accrescere la propria credibilità presso i potenziali clienti, nelle transazioni telematiche B2B e B2C, che dovessero avvenire per il suo tramite.

Il servizio di certificazione è gestito da enti di varia natura (organizzazioni *no profit*, associazioni di categoria, associazioni di consumatori *etc.*), i quali, poiché sono sprovvisti di pubblici poteri “certificativi”, si limitano ad attestare formalmente la conformità del sito a un insieme di regole, che possono essere di natura legislativa e/o tecnica. Si passa dalla certificazione di siti web in regola con la privacy, o in regola con la normativa europea sull’e-commerce, ad esempio, sino alla certificazione di un processo sicuro di acquisto on line. Del resto, si sa, le truffe via Internet sono ormai una costante. “Siti fantasma” o, semplicemente, poco trasparenti in ordine alle informazioni fornite per la conclusione di un contratto telematico rappresentano le paure più ricorrenti di coloro che diffidano dell’e-commerce e perciò, solo attraverso l’attestazione della corrispondenza di un dato sito a una persona fisica o giuridica, il consumatore può fidarsi, riconoscere il venditore ed essere certo di aver effettivamente a che fare con lui.

Benché non esista ancora un *corpus normativo* omogeneo di norme (analogamente a quelle ISO 9000, sulla certificazione di qualità a livello aziendale), che disciplini e specifichi a livello internazionale quali debbano essere le regole, i requisiti, le caratteristiche che un sito di e-commerce deve possedere per essere certificato, si è comunque giunti all’elaborazione di un nucleo di requisiti minimi ritenuti indispensabili per la credibilità di un sito telematico di commercio elettronico.

In particolare, per quanto concerne, i “certificatori” italiani, essi per giudicare affidabile un sito web, ricavano i propri “criteri-guida” sia dalla normativa italiana che dalle direttive comunitarie emanate in materia di e-commerce, nonché dalla cosiddetta “netiquette”, ossia galateo del Web.

²⁹ Federica Bertoni e Graziano Garrisi in “Le problematiche anazionali dell’Internet”, pubblicato nel Volume “I profili giuridici di un e-shop - Guida pratica alle problematiche legali di un negozio on line”, a cura di A. Lisi, Halley Editrice, 2006.

Il commerciante “certificato”, perciò, nel momento in cui si accinge a presentare le proprie offerte su un sito web, deve fornire all’acquirente informazioni circa:

- la denominazione sociale e il possesso delle autorizzazioni che fossero ritenute indispensabili per legge per lo svolgimento dell’attività;
- i prodotti e i servizi offerti (prezzi, condizioni e tempi di consegna);
- la possibilità offerta al cliente di controllare l’ordine prima della sua emissione;
- le modalità di fatturazione e pagamento;
- la normativa in materia di privacy e di trattamento dei dati personali;
- la possibilità di effettuare pagamenti elettronici in modalità sicura;
- la veridicità di quanto pubblicizzato;
- i recapiti per contattare direttamente il venditore in caso di reclami.

Di conseguenza, poiché le informazioni appena elencate dovrebbero porsi alla base delle garanzie da rintracciare all’interno di un sito web di commercio elettronico, è chiaro che l’utente deve essere conseguentemente messo nella condizione di poterle reperire facilmente, insieme al riferimento al codice di condotta seguito dall’imprenditore, nonché alla certificazione ottenuta. In teoria, questa procedura dovrebbe garantire un buon livello di sicurezza per i cyberconsumatori, ma in realtà presenta una serie di lacune.

Innanzitutto tale forma di certificazione non è obbligatoria: molti siti di e-commerce ne sono dotati, ma non tutti. Il problema più rilevante però riguarda gli stessi **certificatori**. Il certificato rilasciato altro non è che un “marchio elettronico” rilasciato da società private che fanno di questo mestiere il proprio *business*. Per cui la validità legale del certificato è molto relativa ed è sostanzialmente limitata alla regolamentazione contrattuale in vigore tra le parti³⁰. Benché gli enti preposti al rilascio della certificazione possiedano, infatti, un proprio regolamento, affiancato, a volte, da veri e propri codici di condotta (nei quali sono stabilite le regole base sul comportamento da tenere nelle procedure di rilascio della certificazione, nelle procedure di eventuale ritiro del marchio e nella procedura di risoluzione delle controversie) e nonostante tali codici enucleino i diritti e i doveri spettanti al soggetto certificato, l’unica garanzia per il visitatore del sito certificato rimane l’affidabilità del certificatore stesso e il suo effettivo potere formale sul sito liberamente sottoposto al suo controllo. Tuttavia, questi – lo ribadiamo - ha un ruolo esterno e formale e non può, quindi, garantire nulla in merito alla validità giuridica e alla sicurezza dei processi di negoziazione che possono strutturarsi all’interno del sito e che perciò continuano a subire la precarietà normativa dell’incontro virtuale³¹.

Eppure, in una situazione in cui l’utilizzo degli strumenti certificati e legislativamente regolamentati stenta a decollare, la **certificazione sostanziale e tecnica (e, quindi, non solo formale)** dei processi di negoziazione on line, effettuata da **terze parti fidate** di servizi di rilievo nazionale e/o europeo o meglio ancora internazionale, potrebbe portare a garantire una sorta di “validazione legale” dell’intera procedura di e-commerce e, quindi, delle manifestazioni di volontà telematica espresse all’interno delle aree riservate dei siti web.

È forse questa l’ultima frontiera? Per ora, pare proprio di sì.

³⁰ <<Essenzialmente si tratta, in altre parole, di condizioni generali di contratto ai sensi dell’art. 1341 c.c. predisposte dai “certificatori” per regolare i contratti relativi alla prestazione dei servizi relativi al rilascio dei marchi di affidabilità. Come abbiamo visto, infatti, l’attività in esame nasce ad iniziativa di enti “non governativi”, che, pertanto, la regolano secondo il diritto privato. Così, il “certificatore” ed il titolare del sito Web desideroso di ottenere una “certificazione”, stipulano un contratto “atipico” ex art. 1322 cpv. c.c. La causa del contratto può essere identificata, essenzialmente, nella concessione di un marchio di affidabilità da parte dell’ente, con relativo diritto-obbligo del titolare del sito di posizionarlo nell’home page del proprio sito, e obbligo di quest’ultimo di attenersi a determinate regole comportamentali. Concluso il contratto, i soggetti risultano vincolati alle varie statuizioni contenute nel contratto stesso, nel regolamento, nel codice di condotta e in altri eventuali documenti. Pertanto qualora uno dei soggetti non si attenga a tali regole, l’altro può senz’altro agire ex art. 1218 c.c.>>, Avv. Fabrizio Macrì, *La “certificazione” dei siti web*, <http://www.filodiritto.com/diritto/privato/informaticagiuridica/certificazioniesitiwebmacri.htm#2>

³¹ Cfr. sent. Cass. 11445/2001

Con i certificatori di processi di negoziazione telematica, infatti si possono garantire servizi di certificazione sufficientemente sicuri, idonei a validare i dati informatici scambiati all'interno di un sito di e-commerce e si possono sviluppare, nell'area riservata alla transazione commerciale, **documenti informatici statici non modificabili** e **documenti da portare in conservazione sostitutiva automatica**, ai sensi delle disposizioni di legge e secondo quanto riferito dalla deliberazione CNIPA n. 11 /2004³².

In particolare, il mercato virtuale dovrà necessariamente affidarsi a sistemi di certificazione, internazionalmente riconosciuti, che permettano di autenticare gli eventi in Rete, attraverso meccanismi di **strong authentication, protocolli informatici sicuri e sistemi di firma elettronica applicata agli hash delle transazioni** che siano in grado di dare certezza e sicurezza:

- alla **trasmissione di dati** verso una **precisa destinazione in data e ora determinate**;
- all'identità del **mittente** e del **destinatario** di tali dati digitali;
- all'**autenticità** di determinati **dati digitali**;
- all'**esistenza di determinati dati digitali** in un dato momento.

L'utilizzo di questi sistemi di certificazione (utilizzo combinato di certificazione del sito e della trasmissione dei messaggi di posta elettronica) permette ai processi amministrativi di aziende ed enti pubblici di godere di una notevole semplificazione e, al contempo, sicurezza. In questo modo risulterà essere più agevole per enti pubblici e privati:

- certificare il **workflow di e-invoicing** (e-billing);
- certificare il **processo di negoziazione**, compresi i documenti coinvolti;
- eliminare la necessità di documentazione cartacea nel processo amministrativo a esclusivo scopo di conformità;
- dimostrare il **regolare aggiornamento dei libri contabili** e documenti finanziari simili di un'azienda;
- **certificare i dati digitali**, anche dopo diverso tempo dalla loro archiviazione.

Tuttavia chi scrive è dell'avviso che, nonostante la certificazione possa essere definita l'ultima frontiera in termini di sicurezza e validazione dei dati di natura commerciale e, quindi, sia stato compiuto un innegabile passo in avanti per il futuro del commercio elettronico, il problema dell'individuazione delle terze parti fidate preposte alla certificazione delle transazioni telematiche permane. E' indispensabile, in una materia così delicata come questa, ipotizzare una sinergia di competenze diverse e trasversali pronte a rispondere con chiarezza e concretezza alle nuove problematiche che la Società dell'Informazione propone; il mercato virtuale avverte con forza la necessità di una nuova *equipe* di saperi, in cui tecnici del diritto e informatici, lavorando gomito a gomito, possano concretamente attribuire ai processi telematici la validità legale e sostanziale di cui oggi, in Internet, si sente sempre più bisogno.

³² Così Avv. Andrea Lisi, *abstract* tratto dagli atti del Convegno "Dalla lex mercatoria alla lex electronica nell'architettura dell'e-business: opportunità, questioni legali e tecnologiche applicate al mercato" tenutosi a Santa Margherita Ligure (GE), 5 - 6 MAGGIO 2006, http://www.scint.it/news_new.php?id=752