Firma Elettronica Non Avanzata
Una personale opinione sulla c.d. “firma elettronica debole”.

III) FIRMA ELETTRONICA c.d. “debole” (NON AVANZATA)

Come in altri scritti in corso di pubblicazione, anche in questo caso cercherò di attenermi allo stretto dato testuale della legge, nell’intento di procedere ad una lettura strettamente legata al testo, che possa ricondurre l’interpretazione della norma in senso unitario.

Inoltre volutamente tralascio l’analisi dell’aspetto probatorio dei documenti generati e sottoscritti con i vari tipi di “firme”, aspetto che tratterò con successivo articolo.

Esaminiamo le definizioni risultanti dal DPR 445/2000, norma regolatrice in materia:

Art.1, lettera b):
b) DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
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;
cc) FIRMA ELETTRONICA ai sensi dell'articolo 2, comma 1, lettera a), del decreto legislativo 23 gennaio 2002, n. 10, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
dd) FIRMA ELETTRONICA AVANZATA ai sensi dell'articolo 2, comma 1, lettera g), del decreto legislativo 23 gennaio 2002, n. 10, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
ee) FIRMA ELETTRONICA QUALIFICATA la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

SEZIONE II
DOCUMENTO INFORMATICO

Articolo 8 (R) Documento informatico
1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico.

Articolo 10 (R) Forma ed efficacia del documento informatico
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 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 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.
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.
5. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su di 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 Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Comunità 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 la Comunità e Paesi terzi o organizzazioni internazionali.
6. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro dell'economia e delle finanze.

Ritengo che, sostanzialmente, l'attenzione si debba concentrare soprattutto su due termini / aspetti della questione, ed esattamente:

1. il significato da attribuire all'espressione "*autenticazione informatica*"
2. il significato da attribuire all'espressione "*Il documento informatico, sottoscritto con firma elettronica…*".

Preliminarmente occorre chiarire che il secondo comma dell'art.10 del DPR 445/2000 fa riferimento ad un concetto di "sottoscrizione" che non coincide esattamente con la sottoscrizione tipica del nostro diritto (ovvero quella autografa, alla quale fa invece riferimento il successivo comma terzo del medesimo articolo), e che il documento (informatico) risultante dalla procedura sarà scritto (ovvero avrà lo "status giuridico" di forma scritta, e quindi "non orale") – in quanto "sottoscritto con firma elettronica [semplice]" – ma non risulterà sottoscritto, in alcun modo, con firma autografa, con tutte le implicazioni che la legge fa – eventualmente - conseguire nei casi di specie.

Ricordo ancora un principio assolutamente generale dell'ordinamento italiano: la forma scritta per i contratti non è la norma, è l'eccezione. Molti contratti possono essere validamente stipulati in forma orale; ben altra questione è la possibilità di "dimostrare" l'esistenza di un determinato accordo o contratto, questione che – come è noto – attiene all'aspetto probatorio relativo al contenuto del documento.

Altro aspetto ancora ulteriore, strettamente connesso alla validità probatoria del documento, sono i metodi utilizzabili per dimostrare una violazione della formazione della volontà ovvero per dimostrare la non conformità della scrittura alla volontà delle parti, aspetto che anche in questo caso ritengo opportuno esaminare nell'articolo che seguirà e che riguarderà l'efficacia probatoria, positiva e negativa", del documento "scritto" e sottoscritto con le varie forme di "firma elettronica".

L'accordo – suggellato da un documento "scritto" – dovrà / potrà poi essere fatto proprio dalle parti con una sottoscrizione autografa, ovvero con l'equivalente "informatico" della medesima; in pratica, una cosa è affermare che un documento è "scritto" (e quindi – ovviamente - non orale, con quello che ne consegue anche in ordine alle limitazioni della ammissibilità delle prove per testi) e ben altra cosa è affermare che quello medesimo documento possa essere univocamente collegato, come espressione di volontà, ad un determinato soggetto giuridico.

Ciò ribadito, partendo dal principio, la definizione del semplice documento informatico – ovvero del documento esistente solamente in forma "informatica" – è "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"; conseguentemente, si prescinde dalla forma del documento, ma si pone l'accento sul fatto che "in" o "per mezzo" di tale documento, proprio perché informatico e pertanto multiforme, vi possa essere la più varia rappresentazione della realtà.

Tralascio – lo ribadisco ancora - volutamente ogni ragionamento concernente la validità probatoria, che attiene ad altro ambito.

Veniamo alla definizione della c.d. "firma elettronica semplice", o <u>firma elettronica</u> "tout court" così come è chiamata dal DRP 445/2000: "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.*"

La conseguenza logica, giuridica ma anche informatica – nel senso che cercherò di spiegare qui di seguito – è che devono esistere alcune "condizioni" (tutte e contemporaneamente, una sorta di "and"[1] giuridico) affinché si parli di "sottoscrizione" [2]; pertanto, **occorre che**:

1. vi sia un insieme di dati
2. tale insieme di dati sia, tramite associazione logica:
   a. allegato
   b. connesso

   ad altri dati elettronici
3. i dati di cui al punto (1), connessi mediante i metodi descritti al punto (2) ad altri dati elettronici, siano utilizzati come "metodo di autenticazione informatica".

A questo punto non è possibile prescindere, per la soluzione del problema, dalla definizione (che ovviamente troveremo solamente nel mondo dell'informatica) di cosa sia un "metodo di autenticazione informatica":

authentication (da www.webopedia.com)

The process of identifying an individual, usually based on a username and password.
In security systems, authentication is distinct from authorization *, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.*

Quindi, nell'ambito del sistema giuridico italiano, esiste un qualcosa che si attaglia alla descrizione sopra riportata, ed esattamente sono le c.d. "credenziali di autenticazione" ed il "sistema di autorizzazione" previsti dal disciplinare tecnico [3] del dlgs n.196/2003 in materia di trattamento dei dati personali, con l'avvertenza che, però, in questo caso tali termini sono da considerarsi utilizzati – fondamentalmente - per consentire l'accesso ad un "trattamento", e quindi – per logica conseguenza – ad una applicazione informatica che consenta tale

---

[1] Nel senso di operatore booleano

[2] Pur non in termini corretti per il diritto italiano, in quanto la sottoscrizione vera e propria è solamente quella autografa, che viene regolata e specificata in altra parte dell'art.10 del DPR 445/2000, esattamente il comma terzo

[3] Sistema di autenticazione informatica (allegato B del TU 196/2003)

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

trattamento, E NON per la sottoscrizione di qualsivoglia tipologia di documento informatico.

Per precisare quali siano tali credenziali, si rammenta che esse possono consistere:

a) user id e password (*codice per l'identificazione dell'incaricato associato a una parola chiave riservata)*
b) token (*dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato),* eventualmente associato (in alternativa tra loro) a:
    a. *un codice identificativo*
    b. *una parola chiave*
c) una caratteristica biometrica dell'incaricato eventualmente associata (in alternativa tra loro) a:
    a. *un codice identificativo*
    b. *una parola chiave*

Orbene, come ho appena precisato, tali "credenziali" sono quelle tipiche che consentono di accedere ad un qualunque sistema informatico ovvero ad una qualunque applicazione, ma non costituiscono dei dati che, mediante un sistema di autenticazione informatica, permettano di **sottoscrivere** un documento.

Tipicamente le procedure c.d. di "autenticazione" sono utilizzare per poter accedere ad un sistema informatico, ad una sotto parte di esso, ad applicazioni funzionanti su tale sistema.

Semmai, permettono di attivare l'applicazione che poi apporrà un "qualcosa" al documento medesimo, ovvero permetterà di fare un qualcosa con i dati, ovvero ancora permetterà di spedire una e-mail, ma non permettono di creare una associazione diretta (non parlo di sicurezza, parlo di connessione pura e semplice, anche logica) tra tali credenziali (quindi con il metodo di autenticazione) ed il documento informatico prodotto.

In buona sostanza, riporto qui di seguito alcune email, per cercare di chiarire quanto appena scritto (compresi gli header del messaggio):

A) messaggio inviato a me stesso

Date:?tu?, 3 Feb 2004 10:38:29 +0100
From: Luca de Grazia <luca@degrazia.it>
X-Mailer: The Bat! (v2.01) Business
Reply-To: Luca de Grazia <luca@degrazia.it>
X-Priority: 3 (Normal)
Message-ID: <163845139.20040203103829@degrazia.it>
To: luca@degrazia.it
Subject: Messaggio di prova e-mail come prova scritta
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit
Data ed ora di questo messaggio: martedì 3 febbraio 2004 ore 10.38.01
Da : Luca de Grazia
A : Luca@degrazia.it
OGGETTO: Messaggio di prova e-mail come prova scritta
Luca-M. de Grazia

Avvocato - Patrocinante in Cassazione
http://www.degrazia.it
ICQ:12969258
PGP Key (DSS/RSA) su http://www.degrazia.it/infodirnet/chiavi.htm
---

Credenziali: nessuna
Header: 1 elemento di connessione logica, quindi non "autenticazione informatica".

B) messaggio di cui sopra inviato a me stesso e ricevuto

R?tu?n-Path: <luca@degrazia.it>
Received: from ppp-12.seeweb.it (ppp-12.seeweb.it [212.25.170.140])
by web-02.seeweb.it (8.11.6p2/8.9.3) with ESMTP id i139WP313988
for <luca@degrazia.it>;?tu?, 3 Feb 2004 10:32:26 +0100
Date:?tu?, 3 Feb 2004 10:38:29 +0100
From: Luca de Grazia <luca@degrazia.it>
X-Mailer: The Bat! (v2.01) Business
Reply-To: Luca de Grazia <luca@degrazia.it>
X-Priority: 3 (Normal)
Message-ID: <163845139.20040203103829@degrazia.it>
To: luca@degrazia.it
Subject: Messaggio di prova e-mail come prova scritta
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit
St?tu?:
Data ed ora di questo messaggio: martedì 3 febbraio 2004 ore 10.38.01
Da : Luca de Grazia
A : Luca@degrazia.it
OGGETTO: Messaggio di prova e-mail come prova scritta
Luca-M. de Grazia

Avvocato - Patrocinante in Cassazione
http://www.degrazia.it
ICQ:12969258
PGP Key (DSS/RSA) su http://www.degrazia.it/infodirnet/chiavi.htm
---

Credenziali: user id e password ma per “scaricare la posta”, non per inviarla
Header: 1 elemento di connessione logica, quindi non “autenticazione informatica”.

C) messaggio inviato a me stesso ma “firmato” con PGP

Date:?tu?, 3 Feb 2004 10:43:19 +0100
From: Luca de Grazia <luca@degrazia.it>
X-Mailer: The Bat! (v2.01) Business
Reply-To: Luca de Grazia <luca@degrazia.it>
X-Priority: 3 (Normal)
Message-ID: <1624135366.20040203104319@degrazia.it>
To: luca@degrazia.it
Subject: Messaggio di prova e-mail come prova scritta
Resent-from: Luca de Grazia <luca@degrazia.it>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Data ed ora di questo messaggio: martedì 3 febbraio 2004 ore 10.38.01

Da : Luca de Grazia
A : Luca@degrazia.it

OGGETTO: Messaggio di prova e-mail come prova scritta

Luca-M. de Grazia

- ---------------------------------------
Avvocato - Patrocinante in Cassazione
http://www.degrazia.it
ICQ:12969258
PGP Key (DSS/RSA) su http://www.degrazia.it/infodirnet/chiavi.htm
- ---------------------------------------

-----BEGIN PGP SIGN?tu?E-----
Version: PGP SDK 3.0.3

iQA/AwUBQB9tLqx3nkxJ4HZKEQKB5QCgsa3xzFVJv/xFLtVLvPyaZOSIaYcAoPgh
5eK9FNw+PiP2pANvSGHedp6x
=cyco
-----END PGP SIGN?tu?E-----

Credenziali: nessuna
Header: 1 elemento di connessione logica, quindi non "autenticazione informatica".
Firma generata da PGP: elemento logicamente connesso al documento in maniera non eludibile, generato attraverso una ulteriore coppia di credenziali utilizzate per poter far funzionare il programma medesimo

D) messaggio di cui sopra inviato a me stesso e ricevuto

R?tu?n-Path: <luca@degrazia.it>
Received: from ppp-12.seeweb.it (ppp-12.seeweb.it [212.25.170.140])
by web-02.seeweb.it (8.11.6p2/8.9.3) with ESMTP id i139bF315162
for <luca@degrazia.it>;?tu?, 3 Feb 2004 10:37:16 +0100
Resent-Date:?tu?, 3 Feb 2004 10:37:16 +0100
Resent-Message-Id: <200402030937.i139bF315162@web-02.seeweb.it>
Date:?tu?, 3 Feb 2004 10:43:19 +0100
From: Luca de Grazia <luca@degrazia.it>
X-Mailer: The Bat! (v2.01) Business
Reply-To: Luca de Grazia <luca@degrazia.it>
X-Priority: 3 (Normal)
Message-ID: <1624135366.20040203104319@degrazia.it>
To: luca@degrazia.it
Subject: Messaggio di prova e-mail come prova scritta
Resent-from: Luca de Grazia <luca@degrazia.it>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: 8bit
St?tu?: O

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Data ed ora di questo messaggio: martedì 3 febbraio 2004 ore 10.38.01

Da : Luca de Grazia
A : Luca@degrazia.it

OGGETTO: Messaggio di prova e-mail come prova scritta

Luca-M. de Grazia
- ---------------------------------------
Avvocato - Patrocinante in Cassazione

http://www.degrazia.it
ICQ:12969258
PGP Key (DSS/RSA) su http://www.degrazia.it/infodirnet/chiavi.htm
- ----------

-----BEGIN PGP SIGN?tu?E-----
Version: PGP SDK 3.0.3

iQA/AwUBQB9tLqx3nkxJ4HZKEQKB5QCgsa3xzFVJv/xFLtVLvPyaZOSIaYcAoPgh
5eK9FNw+PiP2pANvSGHedp6x
=cyco
-----END PGP SIGN?tu?E-----

Credenziali: user id e password ma per "scaricare la posta", non per inviarla
Header: 1 elemento di connessione logica, quindi non "autenticazione informatica".
Firma generata da PGP: elemento logicamente connesso al documento in maniera non eludibile, generato attraverso una ulteriore coppia di credenziali utilizzate per poter far funzionare il programma medesimo

Nel solo caso di utilizzazione di P.G.P.[4] il sottoscritto ha:
1) utilizzato una password per poter usare il programma medesimo
2) ha utilizzato le caratteristiche del programma al fine di "connettere logicamente" la propria "firma" al documento da firmare

e, **conseguentemente**, ha utilizzato un metodo di autenticazione informatica per collegare le proprie "credenziali" al documento al quale si vuole dare valenza di documento "scritto".

Nei primi due esempi sopra indicati l'accoppiata di user id e password – in realtà – è stata utilizzata solamente nel caso del messaggio ricevuto, in quanto per la spedizione del messaggio "in uscita" non è richiesta alcuna forma di autenticazione, tipicamente, salvo casi di estrema attenzione alle caratteristiche del sistema utilizzato.

Né vale segnalare la possibilità di utilizzare i c.d. "webmail" ovvero semplicemente la possibilità di gestione della casella di posta in modalità IMAP, che non consente di spedire la posta se prima non si è stati "autenticati" dal sistema (ovvero dall'applicazione *posta elettronica*):

Quale potrebbe essere la sostanza del discorso?

A modesto parere di chi scrive è assolutamente necessario che in qualche modo (programma di crittografia a chiave asimmetrica pubblica, certificato digitale di qualunque tipo, applet java, e chi più ne ha più ne metta) si possa avere una **connessione logica e diretta** tra il documento informatico al quale si vuole far assumere "forma scritta" (sempre a prescindere dalla validità probatoria di tale documento [5]) e tali dati, che – ricordo – devono costituire un "metodo di autenticazione informatica".[6]

Infatti, gli elementi ai quali si fa riferimento (tipicamente, l'utilizzazione di una user id ed una password per attivare l'applicazione [mailer di posta] per spedire il messaggio, nonché gli altri elementi [header messaggio]) non rientrano nel concetto espresso dalla legge ed appena descritto; costituiscono, semmai, elementi probatori (peraltro anche non troppo facili da porre nel nulla) nel

[4] Pretty Good Privacy, www.pgp.com, programma di cifratura a chiave asimmetrica.
[5] *Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.(secondo periodo dell'art.10 de DPR 445/2000)*
[6] Pertanto, con riferimento alla notizia pubblicata su http://www.studiumfori.it/visallex.php?id=1474 (Ingiunzione di pagamento: il messaggio e-mail è prova scritta), pur complimentandomi con il collega ed amico Marco Cuniberti in quanto ha saputo – quanto meno – "smuovere" un organo giudicante e porre il medesimo di fronte al problema, devo dire che non concordo assolutamente con la tesi sostenuta nel ricorso.

caso in cui l'eventuale opponente contesti il contenuto di tali messaggi e-mail, ma non costituiscono *"l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"*.

Qualche esempio di utilizzazione pratica anche della firma "debole" si potrebbe comunque conseguire (a prescindere da quanto disposto di recente dalle regole sulla archiviazione elettronica dei documenti) in tutti i quei casi in cui occorra "documentare" una "espressione del consenso", ovvero in tutti i quei casi in cui per la validità di un contratto occorre solamente l'incontro della volontà delle parti, e non anche la "sottoscrizione autografa" del medesimo.

In buona sostanza, tutti i contratti che possano essere stipulati in forma "orale" potranno tranquillamente essere stipulati attraverso l'utilizzo della firma elettronica "debole", così come quelli che potranno essere redatti "per iscritto" ma "ad probationem" [7], mentre i casi in cui il contratto debba avere la forma scritta "ad substantiam"[8], forma scritta che debba essere "avallata" da una "sottoscrizione autografa", la firma elettronica semplice non potrà essere utilizzata.

Probabilmente il nodo principale da chiarire, in via interpretativa, legislativa o giurisprudenziale, è proprio questo; occorre poter rispondere alla domanda "*quando è necessaria nel diritto italiano la sottoscrizione autografa?"*. In tutti i casi in cui sia necessaria tale forma di sottoscrizione [9], allora non potrà essere utilizzata la c.d. "firma elettronica debole"; in tutti gli altri casi, si.

Mi sembra che a tale domanda possa essere data una risposta parziale riprendendo il ragionamento effettuato dalla S.C.[10]; nella sentenza indicata in nota, abbastanza recente, la S.C. sembra ritenere necessario che tutti gli elementi di un contratto nel quale sia richiesta la forma scritta "*ad substantiam*" debbano essere, appunto, evidenziati per iscritto. Da tale assunto, dovrebbe discendere come logica conseguenza che anche la sottoscrizione del documento non possa essere che quella autografa, a prescindere dalla successiva qualificazione giuridica dell'atto (scrittura privata, scrittura riconosciuta ovvero atto pubblico).

Ulteriore riprova del ragionamento appena effettuato può essere ritrovato nella massima riportata in nota [11], nella quale si fa espresso riferimento – anche per collegare la volontà delle parti al contenuto degli atti – alla sottoscrizione autografa, che in alcun modo, allo stato attuale della legislazione in campo "informatico", può essere collegata alla firma elettronica che non sia **almeno qualificata.**

A mero titolo esemplificativo mi sembra opportuno notare che l'esempio tipicamente portato a sostegno del ragionamento contrario a quello appena espresso (utilizzazione del bancomat), nasce da alcuni presupposti assolutamente errati; ed infatti, brevemente:

1. il bancomat viene rilasciato dopo la sottoscrizione (su carta) di uno specifico contratto con il soggetto che – conseguentemente - fornisce lo strumento per prelevare denaro;
2. nel caso di "utilizzazione" del bancomat siamo in presenza della utilizzazione della tipologia di credenziali di cui al punto (b) sopra specificato[12], in quanto siamo in possesso di un

---

[7] Come si suole dire, per provare che gli accordi fossero quelli scritti nel contratto

[8] Nel senso che se NON è scritto il contratto non ha valore

[9] Che corrisponde, nell'informatica, alla firma digitale e che può corrispondere a quella elettronica avanzata con determinate caratteristiche

[10] *"….infatti, per il trasferimento della proprietà immobiliare mediante contratto è richiesta, ad substantiam, la forma scritta e questa va riferita a tutti gli elementi fondamentali del negozio, tra i quali è essenziale la volontà attuale delle parti di determinare tale effetto giuridico…."* Cassazione civile, sez. III, 18 giugno 2003, n. 9687 D&G - Dir. e Giust. 2003, f. 28, 106

[11] *L'apposizione del termine al contratto di lavoro, oltre che risultare da atto scritto, deve essere coeva o anteriore all'inizio del rapporto lavorativo, anche se non è richiesto che la dichiarazione di volontà e l'apposizione del termine siano contenuti in un unico documento, in quanto il requisito della* ***forma scritta*** *deve ritenersi osservato anche* ***allorquando la sottoscrizione del lavoratore sia contenuta in un documento a sè****, costituente accettazione di una proposta, anch'essa* ***scritta****, di contratto a termine formulata dal datore di lavoro e il contratto sia concluso, ai sensi dell'art. 1326 c.c., prima o contemporaneamente all'inizio della prestazione. (Nella specie, la S.C. ha confermato la sentenza impugnata che aveva ritenuto illegittima l'apposizione del termine contenuto in una lettera di assunzione non sottoscritta dal lavoratore, il quale ne aveva solo preso conoscenza a seguito di consegna effettuata per conto del datore di lavoro).* Cassazione civile, sez. lav., 11 dicembre 2002, n. 17674 *Soc. Get gestione Esattoria tesoreria liquid. c. Rondinelli Giust. civ. Mass. 2002, 2177*

[12] *token (*dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato), *eventualmente associato (in alternativa tra loro) a:*
un codice identificativo
una parola chiave

“dispositivo” e digitiamo una “password”, credenziali che servono solamente per accedere ad una applicazione che ci consente determinate azioni individuate dal contratto. Conseguentemente non firmiamo alcunché, ma siamo solamente posti in condizione di attivare delle procedure che hanno come “output” – tipicamente – il prelievo di denaro contante ovvero l’ordine di acquisto di determinati servizi.

Ovviamente, sino a quando non vi sarà giurisprudenza conforme sul punto, ovvero una norma chiarificatrice (anche se qualche elemento è possibile ritrovarlo nella proposta di normativa tecnica che dovrebbe sostituire il DPCM 08.02.98), quella esposta rimane solamente una opinione, anche se ritengo sostanzialmente più corretto – soprattutto in fase di “informazione” – non dare per scontato circostanze che potrebbero facilmente essere disattese sia dai fatti, sia da una lettura rigorosa della norma.

Avv. Luca-M. de Grazia