GRUPPO DI INIZIATIVA FORENSE

BANCA POPOLARE DI VERONA
GRUPPO BANCO POPOLARE DI VERONA E NOVARA

CSIG Centro Studi Informatica Giuridica

Convegno

"Documento Informatico: Problematiche di formazione e probatorie"

Col Patrocinio:
dell'Unione Triveneta dei Consigli dell'Ordine Avvocati
dell'Unione Nazionale Camere Civili
dell'A.I.G.A.
dell'Ordine degli Avvocati Verona
dell'Ordine dei Dottori Commercialisti di Verona
del Circolo dei Giuristi Telematici

VERONA 7 MAGGIO 2004

Sala Convegni Banco Popolare di Verona e Novara

Via San Cosimo,10-Verona

Il Convegno si propone di analizzare le recenti problematiche riguardanti il documento informatico. In particolare saranno affrontate, al mattino, le questioni riguardanti gli aspetti penalistici dei reati sui documenti informatici (falso, abuso, diffamazione etc.), quelli procedurali di acquisizione della prova nel processo penale, quelli derivanti dalla recente normativa sulla smaterializzazione delle scritture contabili e quelli connessi alla normativa privacy (corrispondenza, produzione in giudizio e privacy). Nel pomeriggio dopo una introduzione tecnica sul documento informatico, saranno affrontate le questioni connesse al suo valore probatorio e le ulteriori implicazioni connesse alla nuova normativa sulla posta elettronica certificata.

Relazioni :

Scena criminis, documento informatico e formazione della prova penale: dr. Gerardo Costabile, *Member of "The International Association of Computer Investigative Specialists" - Guardia di Finanza di Milano – Circolo dei Giuristi Telematici.*

La fattura elettronica e la "smaterializzazione" delle scritture contabili; profili problematici: avv. Antonino Attanasio, *Avvocato in Cesena, Consulente Tributario e di Diritto delle Nuove Tecnologie - Circolo dei Giuristi Telematici*

Email, documento informatico e privacy: avv. Giulia Ferrarese, *Avvocato del Foro di Verona - Circolo dei Giuristi Telematici*

Efficacia probatoria del documento informatico: dr. Ernesto D'Amico, *Giudice del Tribunale di Verona.*

Azioni di disconoscimento del documento informatico: avv. Marisa Bonanno, *Avvocato del Foro di Verona, curatore responsabile del sito www.studiumfori.it - Circolo dei Giuristi Telematici*

Email e prova nel procedimento monitorio: avv. Luca Giacopuzzi, *Avvocato del Foro di Verona, esperto di problematiche dell'ICT*

Contributi:

Marco Cuniberti, *Avvocato in Cuneo*

Andrea Lisi, *Avvocato in Lecce*

Donato Caccavella, *Esperto in informatica*

Non appena ci saranno giunte, diffonderemo le relazioni del dr. Guido Papalia e dell'avv. Massimo Melica

Un sincero ringraziamento, oltre che ai Relatori, anche al Presidente del Tribunale di Verona – dr. Francesco Abate- ed al VicePresidente dell'Unione Triveneta dei Consigli dell'Ordine degli Avvocati –avv. Giovanni Chiello- che hanno presieduto le due sessioni di lavoro.

Confidiamo che gli stessi siano in streaming visibili quanto prima sul sito web dell'Unione.

La Segreteria Organizzativa (avv. Antonio Rosa)

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO

Problematiche

di formazione e probatorie

Gerardo Costabile

"Scena criminis, documento informatico e formazione della prova penale"

In una posizione particolare, non codificata e non sempre puntualizzata dalla dottrina o dalla giurisprudenza, si pongono le cosiddette *"prove digitali",* in una sorta di *"metaterritorio",* dove sembrerebbe perdere consistenza la naturale propensione dell'uomo di rapportarsi al mondo "*reale*" con l'uso dei cinque sensi e del tatto in particolare.
Questa pseudo-immaterialità nel processo di formazione della prova può dirsi strettamente correlata alla scarsa conoscenza del mondo "digitale", ormai trasversalmente e prepotentemente presente simbioticamente nel mondo "reale", tanto da rendere necessaria una nuova regolamentazione nel settore o, meglio ancora, l'aggiornamento di quella preesistente.

I computer e le altre apparecchiature elettroniche sono ormai presenti in ogni momento della nostra vita. L'uso dei nuovi metodi di comunicazione digitale, come ad esempio internet e le e-mail, ha drammaticamente incrementato l'ammontare delle informazioni che sono ordinariamente conservate e trasmesse solo in forma digitale. Questa evoluzione tecnologica ha però, contestualmente, agevolato e migliorato anche la commissione di vecchi e nuovi reati da parte della criminalità.
I computer, per questo motivo, possono essere i nuovi protagonisti nella commissione di reati, possono contenere le prove per crimini di tipo comune oppure possono essere essi stessi obiettivi di atti criminali. Ed è in tale contesto che si pone il *cyber-investigatore*, il quale ha l'esigenza e il dovere di valutare prima di tutto il ruolo e la natura delle *"impronte elettroniche"*, individuare quali supporti informatici possano contenere potenziali tracce nella *scena criminis*, acquisire e preservare

le stesse fino alla loro successiva analisi, laddove non fosse possibile espletare i dovuti accertamenti direttamente sul posto.

In Italia, purtroppo, non esiste formalmente una standardizzazione delle procedure e le modalità operative vengono demandate alla naturale professionalità degli operatori e della magistratura delegante, tentando affannosamente di non allontanarsi dalla sottilissima linea immaginaria, costituita dai quei principi generali del codice di procedura penale.
L'esperienza processuale ha però talvolta insegnato che è facile trasformare quella padronanza del *thema probandum* in un boomerang, vanificando in dibattimento tutta l'onerosa attività di indagine della fase preliminare.

Ma cosa sono realmente le tracce elettroniche, e particolarmente quelle informatiche? Non esiste una definizione codificata. In generale, quando si parla di *"digital evidence"* si vuole richiamare l'attenzione sulle informazioni ed i dati conservati o trasmessi dalle apparecchiature cosiddette digitali.
Queste tracce, come già accennato, sono caratterizzate da una foggia di immaterialità e per questa loro natura, per così dire aleatoria, possono essere considerate sussumibili alle impronte digitali oppure alle analisi del DNA. Ed è proprio a causa della loro fragilità che tali tracce possono essere facilmente alterate, danneggiate o distrutte, anche per colpa degli stessi investigatori o esaminatori non idoneamente preparati, con la conseguenza di fornire il fianco alla difesa dell'indagato, la quale potrà agevolmente infondere il dubbio alla magistratura giudicante sulla genuinità dell'iter di formazione della prova.

L'irreversibile passaggio dalla carta ai *bits* con la conseguente necessità di dimostrare in sede dibattimentale l'efficacia probatoria delle tracce informatiche e dei significati ad esse ascritti, pone alcuni interessanti interrogativi. Come possiamo garantire l'integrità di queste "*digital evidence*"?

Contrariamente a quanto si pensi, la sensibilizzazione per un comportamento corretto nel maneggiare le nuove tecnologie non è necessaria esclusivamente per le attività di accertamento dei reati informatici in senso stretto, ma appare di notevole importanza anche per quanto attiene altre tipologie di indagine, perfino di natura amministrativo-fiscale.

La cura del personale nell'esecuzione di indagini tipiche di polizia giudiziaria deve essere improntata alla protezione della *scena criminis*[1], al fine di assicurare l'integrità di tutte le prove, che siano esse di tipo tradizionale o elettronico-digitali.

La fase più delicata dell'azione di polizia giudiziaria, quando sono "trattate" informazioni digitali, è quella dell'acquisizione.

E' necessario, infatti, per evitare sgradite sorprese in fase dibattimentale e consentire eventuali perizie di parte su informazioni "genuine", che l'attività di analisi delle tracce informatiche sia operata non sull'originale del supporto sequestrato, ma su di una "*immagine*" dello stesso, consentendo in un secondo momento di effettuare una medesima attività a riscontro delle risultanze investigative ivi compendiate.

La "*bit stream image*", a differenza della mera copia, consentirà di operare su un hard disk praticamente identico all'originale, sia in maniera logica che fisica, quindi anche su eventuali parti presumibilmente vuote dello stesso, che potrebbero contenere *file* o frammenti di *file* cancellati non sempre visibili con i normali strumenti di *windows*[2].

Dovrà essere all'uopo effettuata tale operazione con idonei strumenti, hardware e software, che consentano di mantenere inalterata la traccia informatica oggetto dell'analisi, al fine di evitare dubbi sull'integrità dei dati contenuti nei supporti in parola e previo utilizzo di hard disk nuovo oppure assoggettato ad operazione di *wiper* (trattasi di rimozione dei dati molto approfondita con particolari programmi per evitare che possa essere recuperato un file cancellato riconducibile, ad esempio, al precedente utilizzatore del supporto usato).

Il sistema[3], infine, dovrà operare in maniera non invasiva, ad esempio con l'ausilio di un blocco in scrittura, che consentirà di non compromette l'integrità dei dati contenuti nel supporto oppure anche la mera variazione di un semplice orario di accesso ai file[4], che non sarà ovviamente compatibile

---

[1] Marco Strano, Relazione alla Conferenza sul Cybercrime, Palermo, 3-4-5 Ottobre 2002, dove l'autore individua il *cyber-criminale* proiettato *"in un contesto digitale, laddove la scena criminis (il luogo del delitto) si localizza tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del monitor"*.

[2] In tal modo viene anche preservata l'allocazione dei singoli file sul supporto originale. Infatti se vengono copiati i dati di un hard disk su un altro supporto idoneo, con un semplice procedimento di copia, i dati presenti in entrambe i dischi saranno uguali, ma sarà diversa la loro distribuzione.

[3] Il software che ad oggi sembrerebbe quello più utilizzato per l'analisi in parola si chiama *EnCase,* prodotto dalla *Guidance Software,* destinato all'uso professionale ed investigativo da numerose agenzie e forze dell'ordine in tutto il mondo e considerato in linea con gli standard internazionali per le analisi delle tracce informatiche. Qualche critica è stata formulata dai promotori dell'*open source*, in quanto non sarebbero disponibili i codici sorgenti del software e quindi non sarebbe trasparente la procedura di *working* dell'analizzatore. Altri software di pregio utilizzati dagli esperti sono, tra gli altri, "SMART" e "Ilook investigator", quest'ultimo ad uso esclusivo delle forze dell'ordine, dei militari e delle agenzie governative su scala internazionale.

[4] Per questo motivo è vivamente sconsigliabile l'accensione dei computer durante l'attività di sequestro, se lo stesso è spento. In tutti i casi comunque è indispensabile operare con la continua assistenza della parte, verbalizzando con precisione gli orari, tra i quali potrebbe essere importante riportare quello indicato dal computer stesso, evidenziando l'eventuale disallineamento.

con quello dell'avvenuto sequestro e quindi potrebbe compromettere l'eventuale non-ripudiabilità delle citate informazioni.

Nella formazione dell'immagine dovrà essere creata anche una sorta di impronta, che contraddistinguerà in maniera univoca la traccia informatica oggetto dell'analisi forense, al fine di ottemperare alle citate esigenze di integrità del dato. Tale "marchio digitale" sarà creato con un'operazione cosiddetta di *hashing* a senso unico, con algoritmo di classe MD5, che genera un'impronta della lunghezza di 128 bit (16 byte). L'impronta costituisce un riferimento certo alla traccia originale, ma non ne consente la ricostruzione. Tale algoritmo è utilizzato a livello internazionale e garantisce un buon livello di sicurezza. Difatti la probabilità di avere la medesima impronta per due documenti differenti, anche se solo di una virgola, è pari a 2 elevato alla 128^ potenza, ovvero sarebbe ad esempio come vincere il granpremio americano della lotteria Powerboll per 39 volte di seguito.

Più in generale il mondo giuridico e giudiziario appare diviso sulla necessità o meno di acquisire tutto il supporto informatico nella fase di sequestro penale. Molteplici sono state le posizioni, più o meno condivise dalla giurisprudenza, di coloro che indicavano come oggetto del sequestro non il contenitore in se, ma i dati informatici ivi contenuti. Le critiche più articolate, da parte della dottrina[5], hanno preso le mosse da un attento esame dell'istituto del sequestro probatorio, approfondendo le nozioni di corpo del reato e cose pertinenti al reato. Infatti l'art. 253 comma 2 cpp indica quale corpo del reato quelle cose sulle quali o mediante le quali il reato è stato commesso, includendo altresì quelle che ne costituiscono il prodotto, il profitto o il prezzo.

Secondo la citata dottrina, non sarebbe conciliabile la definizione marcatamente materiale del legislatore con la natura immateriale delle tracce informatiche[6].

D'altro canto la giurisprudenza non sembra aver dato adeguate risposte, riconoscendo alternativamente ad un computer[7] la qualità di corpo del reato, ovvero il mezzo attraverso il quale viene consumata l'azione criminosa, oppure di cosa pertinente al reato, in quanto elemento esterno dell'*iter criminis*, con l'esame del quale può essere dimostrato il fatto criminoso, comprese le modalità di preparazione ed esecuzione[8].

E' palese che tale vincolo pertinenziale non sembra sussistere sempre tra il reato e l'intero supporto informatico, in luogo delle sole tracce ivi contenute, almeno nei casi in cui il computer non può essere semplicisticamente considerato come "l'arma del delitto".

---

[5] Cfr. Francesco Marcellino, Principio di pertinenza e sequestri di computer, disponibile su www.netjus.org.

[6] L'immaterialità del dato informatico è stata riconosciuta dallo stesso legislatore il quale, tra i computer crimes, non ha previsto il reato di furto, limitandosi alla mera duplicazione abusiva.

[7] Cfr. Cass. Pen Sez. VI, 29 gennaio 1998.

[8] Cfr. Cass. Pen. Sez. V, 22 gennaio 1997, n. 4421.

Per questo motivo appare fondamentale valutare il "ruolo" del computer nell'attività illecita, per motivarne l'eventuale sequestro.

In generale infatti l'hardware di un computer può essere osservato sotto due distinti profili. Il computer, e non solo quello ovviamente, può assumere la veste di mero contenitore della prova del crimine, ad esempio può immagazzinare il piano di una rapina o le mail intercorse tra i complici. In tal caso non sarà necessaria un'azione di sequestro, ma potrà essere operata in contraddittorio una semplice masterizzazione delle tracce pertinenti al reato, con lo strumento di polizia giudiziaria più appropriato, come ad esempio un'ispezione delegata ex art. 246 cpp.

L'ispezione è una particolare attività tipica di polizia giudiziaria volta all'esame di persone, cose o luoghi, allo scopo di accertare le tracce e gli altri effetti materiali del reato (ad esempio impronte sul pavimento, macchie di sangue).

Questa attività di polizia giudiziaria, poco utilizzata nel settore dei reati informatici in quanto esigente di specifiche competenze tecniche e variegato materiale software, è caratterizzata dall'irripetibilità degli atti, con la conseguente utilizzabilità piena originaria nel dibattimento.

Tale procedura, molto incoraggiata da parte della dottrina, appare consigliabile esclusivamente per piccoli reati (ad esempio in presenza di *dialer*, diffamazione, *virus*), in quanto, come già accennato, si tratta di un'attività particolarmente tecnica dove l'operatore deve, in contradditorio con la parte, "esplorare" i supporti informatici dell'indagato, (o talvolta dello stesso esponente) alla ricerca di dati e tracce informatiche inerenti i fatti oggetto dell'ispezione, che saranno cristallizzati con i dovuti metodi in supporti durevoli allegati al verbale.

Pare meritevole ivi segnalare due limiti: uno di natura meramente temporale, in quanto non è sempre possibile analizzare sul posto una grande mole di dati, considerando anche quelli cancellati che dovranno, ove possibile, essere opportunamente recuperati.

Un altro problema invece è l'impossibilità, da parte dell'indagato, di esperire in un secondo momento una nuova analisi ad opera di un perito di parte, in quanto il supporto prodotto in sede di ispezione, oppure l'hard disk stesso oggetto dell'attività, non saranno i medesimi sui quali il "cyber-investigatore" aveva operato[9].

Dovrà quindi essere valutata preventivamente l'opportunità dell'ispezione, consigliabile preferibilmente quando un sequestro indiscriminato sarebbe sproporzionato al fatto contestato, ovvero quando l'hard disk è stimabile solo come contenitore di documenti informatici inerenti alle indagini, oppure nel caso di attività presso terzi (banche, provider, etc.) estranei di fatto alla vicenda.

---

[9] In realtà tali operazioni di polizia giudiziaria non sono quasi mai oggetto di contestazione immediata da parte dell'indagato il quale, specialmente per reati comuni, non sempre ha la competenza tale per poter contraddire un processo di estrapolazione dei dati, condizionato talvolta anche da una sorta di timore reverenziale.

In altri casi, invece, l'hardware può essere considerato come frutto dell'attività criminale, come ad esempio il contrabbando, oppure uno strumento per la commissione di reati.
Un computer utilizzato per consumare il reato di cui all'art. 615 ter cp (accesso abusivo ad un sistema informatico) potrebbe quindi essere annoverato tra gli strumenti per la commissione del crimine. In America, in questi casi, il *Federal Rule of Criminal Procedure n. 41* consente agli agenti, previo decreto, il sequestro dell'intero hardware, qualunque sia il materiale ivi contenuto. Successivamente sarà effettuata la *digital analysis* del contenuto delle risorse informatiche dell'indagato.
Paradossalmente in Usa sarebbe possibile sequestrare un'intera rete informatica laddove fosse accertata la commissione di un reato ad opera di un amministratore di rete nell'esercizio della propria attività[10].
Negli altri casi, cioè quando l'hardware è un mero contenitore, le procedure federali d'oltreoceano danno maggiore rilevanza al sequestro del dato informatico, ritenuto centrale rispetto all'indagine, rispetto all'hardware che lo contiene. Ciò non vuol dire che il sequestro *tout court* degli hard disk sia vietato, ma viene valutata caso per caso la fattibilità in determinate circostanze "informatiche", ovvero quando la mole di dati è di un certo spessore[11], oppure si ha motivo di ritenere che ci siano file nascosti, stenografati, crittografati, non allocati, ovvero sistemi di autodistruzione dei dati in caso di password errata, etc.

La risposta più adeguata alle problematiche sopra evidenziate sembrerebbe essere il buon senso, ossia garantire una blindatura delle procedure e della relativa *chain of custody,* utilizzando lo strumento giuridico più adatto, motivando adeguatamente la sussistenza delle concrete esigenze probatorie con riferimento, cioè, alla "pertinenza" probatoria delle cose eventualmente sequestrate o oggetto di ispezione, in relazione alle quali andranno indicati gli elementi di fatto specifici che giustificano il provvedimento[12].
Dovrà quindi essere individuato[13] compiutamente il *thema probandum*, ovvero il fatto storico e concreto riconducibile, almeno astrattamente, ad una fattispecie criminosa. In mancanza di tale individuazione non sarebbe possibile accertare né l'esistenza delle esigenze probatorie su cui si fonda il provvedimento, né la natura di corpo del reato o cosa ad esso pertinente, oggetto di ricerca

[10] Trattasi di una facoltà in capo alla polizia giudiziaria americana. Anche in Italia è guardata con più rigore l'opera criminale dell'amministratore di sistema, il quale è punito più severamente in caso ad esempio di accesso abusivo ex art. 615 ter cp.
[11] Questo è il caso più frequente in quanto l'attività di estrapolazione o di *bit stream image* può essere onerosa, dal punto di vista temporale, e in taluni casi può essere più invasiva dell'asportazione dei supporti informatici, che potranno essere "copiati" in laboratorio.
[12] Cfr. Cass. Penale n. 649 del 2 marzo 1995.

e acquisizione. In tal caso quindi la perquisizione non sarà più un mezzo di ricerca della prova, ma un discusso mezzo di acquisizione della *notitia criminis*[14].

Tale indeterminatezza, accompagnata dall'indicazione che potrà essere oggetto di sequestro "quanto ritenuto utile ai fini dell'indagine", rimetterebbe alla polizia giudiziaria la valutazione e l'individuazione dei presupposti fondamentali del sequestro[15], con la spiacevole conseguenza, non avendo ben precisato l'importanza di taluni dati in luogo dell'intero supporto e non avendo valutato la possibilità di un'ispezione delegata, di "agevolare" un sequestro indiscriminato di corposo hardware, contenente dati anche di terze persone e quindi poco inerente[16]. Infatti appare palese la multifunzionalità dei supporti informatici, difficilmente vincolati nella loro interezza all'attività illecita[17].

Il sequestro del bene informatico deve pertanto essere valutato caso per caso e non in maniera superficiale, attesa la molteplice destinazione e funzione dello strumento.

Tale impostazione impone un più rigoroso accertamento sulla sussistenza delle finalità probatorie e sugli strumenti tecnico-giuridici più idonei all'attività di cristallizzazione ed assicurazione della prova informatica, **garantendo altresì certezza, genuinità e paternità ai dati informatici**, evitando contestualmente conseguenze altamente afflittive e interdittive, ancorché lesive ed estranee alle esigenze d'indagine[18].

Appare d'obbligo infine citare, proprio nel codice penale, l'art.. 491 bis dove si legge, tra l'altro: *"omissis… A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli"*. Quindi, testualmente, la distinzione tra il documento cartaceo e quello informatico consiste tutta nel supporto contenente i dati: questi, infatti, viene indicato quale equivalente

---

[13] Cfr. Arrigo Daniele**,** Il riesame della perquisizione e del sequestro penale mancanti dell'indicazione del thema probandum, 1999, n. , p.823, Giurisprudenza Italiana a commento di Cassazione VI Sezione, 26 marzo 1997.

[14] Cfr. Cassazione VI Sezione, 26 marzo 1997, che ritiene "insufficiente quale enunciazione, ancorché sommaria e provvisoria, d'ipotesi accusatoria, la mera indicazione, nei provvedimenti di perquisizione e sequestro, degli articoli di legge pretesamente violati, seguiti da una collocazione spazio-temporale così ampia da non apportare alcun contributo alla descrizione del fatto".

[15] Cfr. "Decreti di perquisizione e sequestri ex art. 252 cpp: limiti e discrasie" - Avv. Alfonso Maria Parisi, Patrocinante in Cassazione, su www.penale.it.

[16] L'indeterminatezza dell'indicazione ha come conseguenza diretta la necessità, secondo parte della giurisprudenza (Cfr. Cass. Pen., V, 17 marzo 2000), di una convalida ex art. 355 cpp.

[17] Il Tribunale di Torino, con un notorio provvedimento del 7 febbraio 2000 in materia di sequestro probatorio di hard disk, pur non accogliendo le eccezioni sull'asserita immaterialità delle tracce informatiche, ha ordinato il dissequestro dell'hardware, riconoscendo altresì che questi è cosa pertinente al reato, ma asserendo che le esigenze probatorie potevano essere garantite con l'estrazione dei soli dati oggetto dell'attività illecita, in quanto l'intero supporto conteneva anche informazioni riferibili alla corrispondenza telematica tra l'indagato e terzi, totalmente estranei ai fatti.

[18] Cfr. Cassazione penale, sez. III, 25 febbraio 1995, n. 105, e Tribunale del riesame di Torino, 7 febbraio 2000.

informatico del tradizionale foglio di carta, sul quale un contenuto eventualmente rappresentativo può essere impresso[19].

Questo spinge a valutare l'attività di assicurazione della prova sempre più nella direzione della cristallizzazione del contenitore in luogo del suo contenuto, mentre nel caso dell'informatica le due cose sono facilmente scindibili, pur assicurando medesimo risultato. In conclusione, quindi, se pure da un lato è possibile l'applicazione di un idoneo accorgimento tecnico, rispettoso dei principi costituzionali e garanzia della genuinità della prova, è auspicabile un aggiornamento delle procedure del codice di rito, al fine di svincolare alcune terminologie dall'impostazione profondamente ancorata alla materialità degli eventi[20].

Mentre tale obiettivo, seppure lontano, appare più chiaro e definito all'orizzonte, tanto che anche alcune Università in Italia (cito, per conoscenza personale, l'**Università di Milano con il Prof Ziccardi e quella di Bologna con il Prof. Maioli**) si stanno facendo promotrici, in ambiente certamente scientifico, di progetti di linee guida per le attività di computer e network forensics[21], le attività sono spesso poco omogenee e gli interventi non sempre proficui, oltre che spesso in pregiudizio di alcuni principi fondamentali dell'individuo.

[19] Leggasi l'interessante articolo su http://www.romagna-camerapenale.it/docinformatico.htm relativo al documento informatico.

[20] Tale impostazione è stata già applicata per dipanare un problema analogo afferente il reato di furto ex art. 624 cp, ove è stata parificata a "cosa mobile anche l'energia elettrica e ogni altra energia che abbia valore economico".

[21] L'accezione "Computer Forensics" si riferisce a quella disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine.

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO
Problematiche
di formazione e probatorie

LA FATTURA ELETTRONICA E LA SMATERIALIZZAZIONE DELLE SCRITTURE CONTABILI: PROFILI PROBLEMATICI (avv. Antonino Attanasio)

1. Il quadro normativo: il decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004 (segue)

Il D.M. MEF 23 gennaio 2004 disciplina le modalità di attuazione degli obblighi fiscali inerenti ai documenti informatici e alla loro riproduzione su diversi tipi di supporto ottico o altro tipo di supporto idoneo.

Ai fini tributari, ad eccezione delle scritture e dei documenti rilevanti ai fini delle disposizioni tributarie nel settore doganale, delle accise e delle imposte di consumo di competenza dell'Agenzia delle dogane (ai quali non si applica il decreto stesso), l'emissione, la conservazione e l'esibizione di documenti, sotto forma di documenti informatici, nonché la conservazione digitale di documenti analogici avvengono in applicazione delle disposizioni del D.P.R. 28 dicembre 2000, n. 445, del D.P.C.M.8 febbraio 1999, della deliberazione CNIPA n. 11 del 19 febbraio 2004.

I documenti informatici rilevanti ai fini tributari:
a) hanno la forma di documenti statici non modificabili;
b) sono emessi, al fine di garantirne l'attestazione della data, l'autenticità e l'integrità, con l'apposizione del riferimento temporale e della sottoscrizione elettronica;
c) sono esibiti secondo le seguenti modalità: sono resi leggibili e, a richiesta, disponibili su supporto cartaceo e informatico presso il luogo di conservazione delle scritture, in caso di verifiche, controlli o ispezioni. I documenti conservati possono essere esibiti anche per via telematica secondo le modalità stabilite con provvedimenti dei direttori delle competenti Agenzie fiscali;
d) sono memorizzati su qualsiasi supporto di cui sia garantita la leggibilità nel tempo, purché sia assicurato l'ordine cronologico e non vi sia soluzione di continuità per ciascun periodo d'imposta;
e) devono essere consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione al cognome, al nome, alla denominazione, al codice fiscale, alla partita Iva, alla data o associazioni logiche di questi ultimi.

Il processo di **conservazione** dei documenti informatici termina con la sottoscrizione elettronica e l'apposizione della marca temporale, in luogo del riferimento temporale, sull'insieme dei predetti

documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti o di insiemi di essi da parte del responsabile della conservazione. Il processo di conservazione è effettuato con cadenza almeno quindicinale per le fatture e almeno annuale per i restanti documenti.

La **riproduzione** dei documenti informatici, su supporto idoneo, avviene secondo le modalità di cui all'art. 1, lettere n) e o) della deliberazione CNIPA n. 11/2004, cioè mediante **riversamento diretto** (processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, senza alterare la loro rappresentazione informatica) o **riversamento sostitutivo** (processo che a differenza del precedente altera la rappresentazione informatica).

Il processo di **conservazione digitale** di **documenti e scritture analogici** rilevanti ai fini tributari avviene mediante memorizzazione della relativa immagine, secondo le stesse modalità previste per i documenti informatici e può essere limitato a una o più tipologie di documenti e scritture analogici, purché **sia assicurato l'ordine cronologico delle registrazioni e non vi sia soluzione di continuità per ogni periodo di imposta**.

Il processo di conservazione digitale di **documenti analogici originali** avviene secondo le modalità previste per i documenti informatici e si conclude con l'ulteriore apposizione del riferimento temporale e della sottoscrizione elettronica da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.

La **distruzione** di documenti analogici, di cui è **obbligatoria la conservazione**, è consentita soltanto dopo il completamento della procedura di conservazione digitale.

Entro il mese successivo alla scadenza dei termini stabiliti dal decreto del Presidente della Repubblica n. 322 del 1998, per la presentazione delle dichiarazioni relative alle imposte sui redditi, all'imposta regionale sulle attività produttive e all'imposta sul valore aggiunto, il soggetto interessato o il responsabile della conservazione, ove designato, al fine di estendere la validità dei documenti informatici trasmette alle competenti Agenzie fiscali, l'impronta dell'archivio informatico oggetto della conservazione, la relativa sottoscrizione elettronica e la marca temporale. Con provvedimento le Agenzie fiscali indicano gli ulteriori dati ed elementi identificativi da comunicare unitamente a quelli di cui in precedenza. Le stesse Agenzie rendono disponibile per via telematica la ricevuta della comunicazione effettuata ed il relativo numero di protocollo.

2. (segue): il D.Lgs. 20 febbraio 2004, n. 52

Il D.Lgs. 20 febbraio 2004 n. 52 costituisce attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA.
Viene sostituito l'intero art. 21 del DPR 633/1072 e i punti rilevanti e innovativi rispetto al passato sono i seguenti:

a) per ciascuna operazione imponibile il soggetto che effettua la cessione del bene o la prestazione del servizio emette fattura, anche sotto forma di nota, conto, parcella e simili, o, ferma restando la sua responsabilità, assicura che la stessa **sia emessa dal cessionario o dal committente**, **ovvero, per suo conto, da un terzo;**
b) l'emissione della fattura, cartacea o elettronica, da parte del cliente o del terzo residente in un Paese con il quale non esiste alcun strumento giuridico che disciplini la reciproca assistenza è consentita, a condizione che ne sia data preventiva comunicazione all'amministrazione finanziaria e purché il soggetto passivo nazionale abbia iniziato l'attività da almeno cinque anni e nei suoi confronti non siano stati notificati, nei cinque anni precedenti, atti impositivi o di

contestazione di violazioni sostanziali in materia di imposta sul valore aggiunto. Con provvedimento del direttore dell'Agenzia delle entrate sono determinate le modalità, i contenuti e le procedure telematiche della comunicazione;

c) la fattura si ha per **emessa** all'atto della sua **consegna** o **spedizione** all'altra parte ovvero all'atto della sua **trasmissione** per via elettronica;
d) la fattura é datata e numerata in ordine progressivo per anno solare e contiene le seguenti indicazioni:
    a) ditta, denominazione o ragione sociale, residenza o domicilio dei soggetti fra cui é effettuata l'operazione, del rappresentante fiscale nonché ubicazione della stabile organizzazione per i soggetti non residenti e, relativamente al cedente o prestatore, numero di partita IVA. Se non si tratta di imprese, società o enti devono essere indicati, in luogo della ditta, denominazione o ragione sociale, il nome e il cognome;
    b) natura, qualità e quantità dei beni e dei servizi formanti oggetto dell'operazione;
    c) corrispettivi ed altri dati necessari per la determinazione della base imponibile, compreso il valore normale dei beni ceduti a titolo di sconto, premio o abbuono di cui all'art. 15, n. 2;
    d) valore normale degli altri beni ceduti a titolo di sconto, premio o abbuono;
    e) aliquota, ammontare dell'imposta e dell'imponibile con arrotondamento al centesimo di euro;
    f) numero di partita IVA del cessionario del bene o del committente del servizio qualora sia debitore dell'imposta in luogo del cedente o del prestatore, con l'indicazione della relativa norma;
    g) data della prima immatricolazione o iscrizione in pubblici registri e numero dei chilometri percorsi, delle ore navigate o delle ore volate, se trattasi di cessione intracomunitaria di mezzi di trasporto nuovi, di cui all'art. 38, comma 4, del decreto-legge 30 agosto 1993, n. 331, convertito, con modificazioni, dalla legge 29 ottobre 1993, n. 427;
    h) annotazione che la stessa è compilata dal cliente ovvero, per conto del cedente o prestatore, da un terzo.

Per le operazioni effettuate nello stesso giorno nei confronti di un medesimo destinatario può essere emessa una sola fattura. In caso di più fatture trasmesse in unico lotto, per via elettronica, allo stesso destinatario da parte di un unico fornitore o prestatore, le indicazioni comuni alle diverse fatture possono essere inserite una sola volta, purché per ogni fattura sia accessibile la totalità delle informazioni.

La trasmissione per via elettronica della fattura, non contenente macroistruzioni né codice eseguibile, è consentita **previo accordo** con il destinatario. L'attestazione della data, l'autenticità dell'origine e l'integrità del contenuto della fattura elettronica sono rispettivamente garantite mediante l'apposizione su ciascuna fattura o sul lotto di fatture del riferimento temporale e della firma elettronica qualificata dell'emittente o mediante sistemi EDI di trasmissione elettronica dei dati che garantiscano i predetti requisiti di autenticità e integrità. Le fatture in lingua straniera devono essere tradotte in lingua nazionale a richiesta dell'amministrazione finanziaria e gli importi possono essere espressi in qualsiasi valuta purché l'imposta sia indicata in euro.

Le fatture elettroniche trasmesse o ricevute in forma elettronica sono archiviate nella stessa forma. Le fatture elettroniche consegnate o spedite in copia sotto forma cartacea possono essere archiviate in forma elettronica. **Il luogo di archiviazione delle stesse può essere situato in un altro Stato**, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza. Il soggetto passivo, residente o domiciliato nel territorio dello Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, ivi compresi i certificati destinati a garantire l'autenticità dell'origine e l'integrità delle fatture emesse in formato elettronico siano stampabili e trasferibili su altro supporto informatico.

L'ispezione documentale si estende a tutti i libri, registri, documenti e scritture, compresi quelli la cui tenuta e conservazione non sono obbligatorie, che si trovano nei locali in cui l'accesso viene eseguito, o che sono comunque accessibili tramite apparecchiature informatiche installate in detti locali.

3. Le parti non attuate della direttiva UE Direttiva 2001/115/CE, 20 dicembre 2001, del Consiglio

La direttiva prevede che la fattura possa essere emessa da un terzo, **in nome e per conto** del soggetto passivo; il decreto legislativo invece permette che la fattura possa essere emessa da un terzo **solo per conto** del soggetto passivo.
Nel caso della generazione ed emissione di fatture da parte del cliente, anziché da parte del fornitore cedente i beni o prestatore dei servizi, la direttiva dispone che la compilazione di fatture, da parte del cliente di un soggetto passivo, per le cessioni di beni o le prestazioni di servizi fornitegli da tale soggetto passivo, è autorizzata previo consenso delle parti e purché ogni fattura sia oggetto di accettazione da parte del soggetto passivo che esegue la cessione di beni o la prestazione di servizi. Gli Stati membri sul cui territorio sono effettuate le cessioni di beni o le prestazioni di servizi determinano le condizioni e modalità del consenso preliminare e delle procedure di accettazione tra il soggetto passivo ed il cliente. Il decreto legislativo tace sul punto.
Il ciclo attivo di fatturazione è articolato in due fasi: compilazione/generazione della fattura da un lato e trasmissione della medesima dall'altro. Nel caso di esternalizzazione del servizio (outsourcing), l'outsourcer si può limitare alla trasmissione della fattura oppure gestire anche la fase compilazione/generazione. La direttiva non evidenziava queste due fasi, mentre il decreto legislativo introduce questa distinzione, laddove prevede in fattura l'annotazione che la stessa è compilata dal cliente ovvero, per conto del cedente o prestatore, da un terzo.

4. Aspetti problematici connessi alla fattura elettronica ed alle scritture contabili in generale

Nel complesso sistema di adempimenti che rendono possibile l´applicazione dell'imposta sul valore aggiunto, sulla base delle indicazioni della VI direttiva 17.5.1977, n.77/388/Cee, la fattura costituisce un elemento imprescindibile. La fatturazione assicura, oltre alle tradizionali esigenze di documentazione e di controllo, la creazione del titolo che legittima il cedente o il prestatore ad esercitare la rivalsa e l´ acquirente ad operare la detrazione dell´ imposta che risulta addebitata in fattura. La fattura è il documento fiscale che è alla base dell'impianto amministrativo, contabile, gestionale e finanziario sia dell'impresa che del professionista ed è anche il solo documento che mette in relazione l'imprenditore ed il professionista con fornitori e clienti.

Sotto altro profilo, si osserva che il reddito d'impresa ed il reddito di lavoro autonomo manifestano le loro componenti per mezzo delle scritture contabili, rese obbligatorie sia dalla normativa civilistica che da quella fiscale. La mancata o l'irregolare tenuta delle scritture contabili legittima gli uffici dell'Amministrazione finanziaria a procedere alla rettifica del reddito di impresa e di lavoro autonomo anche sulla base di presunzioni semplici, con facoltà di prescindere in tutto o in parte dalle risultanze del bilancio e delle scritture contabili stesse.

Il D.Lgs. 20 febbraio 2004 n. 52, consente di trasmettere ed archiviare le fatture generate in formato elettronico, senza l'obbligo di stamparle su carta; il D.M. 23 gennaio 2004 consente invece l'archiviazione in formato analogico o digitale delle fatture passive pervenute in cartaceo.

Con ciò si introduce nei processi aziendali e di studio professionale una innovazione che va a modificare l'attuale sistema di contabilizzazione, trasformando la fattura da "documento fiscale" ad "oggetto software fiscale", ovvero un contenitore di dati ed informazioni che permette da un lato l'automazione totale del processo amministrativo, contabile, gestionale e finanziario, dall'altro di implementare la fattura con software, con estrattori automatici di dati e di informazioni e con "intelligent software agents", che effettuano elaborazioni complesse e sofisticate. Sulla scorta delle considerazioni precedenti, si illustrano di seguito alcuni aspetti problematici della normativa citata.

5. Il preventivo "accordo" con il destinatario della fattura

Il D.Lgs. 52/2004 non disciplina le modalità con cui il soggetto che vuol trasmettere in via elettronica la fattura deve accordarsi preventivamente con il destinatario. L'accordo preventivo può realizzarsi mediante l'inserimento, nel generale accordo commerciale tra le parti, di una apposita clausola contrattuale con la quale le parti convengono che la documentazione fiscalmente rilevante sia trasmessa in via elettronica e secondo le regole di cui al D.Lgs. 52/2004. Considerato inoltre che la ricezione di una fattura in formato elettronico potrebbe costituire un oggettivo aggravio per il destinatario, nel caso in cui non sia attrezzato per la gestione informatizzata delle fatture, o addirittura un impedimento per il caso che non possieda un sistema informatizzato ed aperto nel WEB, è opportuno che il "consenso" sia oggetto di specifica sottoscrizione del destinatario, sul modello delle condizioni generali di contratto di cui all'art. 1341 c.c.

6. L'emissione di fattura in mancanza delle condizioni di cui al nuovo art. 21 D.P.R 633/1972

Il nuovo art. 21 D.P.R. 633/1972 dispone, tra l'altro, che la fattura trasmessa in via elettronica non deve contenere macroistruzioni né codice eseguibile; su di essa, o su ciascun lotto di fatture, deve essere apposto il riferimento temporale e la firma elettronica qualificata. Manca tuttavia la previsione espressa di una sanzione nel caso di violazione di tale disposizione. Per individuare la disciplina da applicare occorre distinguere tra violazioni sostanziali e violazioni formali. Le violazioni sostanziali sono quelle che incidono sulla determinazione o sul pagamento del tributo; le violazioni formali sono quelle irrilevanti ai fini della determinazione o del pagamento del tributo. Le violazioni formali però possono essere finalizzate a consentire al contribuente di fruire di indebiti vantaggi patrimoniali e quindi essere idonee ad arrecare pregiudizio all'esercizio dei controlli e degli accertamenti. L'art.10, comma 3, dello Statuto del Contribuente, approvato con legge 27 luglio 2000 n. 212 dispone che le sanzioni non possono essere irrogate quando il comportamento del contribuente "si traduce in una mera violazione formale senza alcun debito di imposta". Il D.Lgs. 26 gennaio 2001, n. 32 ha inserito nell'art. 6 del D.Lgs. n. 472/1997 il comma 5-bis secondo cui "non sono inoltre punibili le violazioni che non arrecano pregiudizio all'esercizio delle azioni di controllo e non incidono sulla determinazione della base imponibile, dell'imposta e sul versamento del tributo". La valutazione degli effetti della violazione del nuovo articolo 21, con particolare riferimento alla mancata apposizione del riferimento temporale e della firma elettronica, nonché all'assenza di codici eseguibili e macroistruzioni, deve essere svolta ex post ed in concreto, sulla base della coesistenza delle due norme citate. L'art. 10, comma 2, Statuto del contribuente, riguarda le violazioni tributarie - formali o sostanziali - che in concreto si traducono in mere violazioni formali, senza alcun debito di imposta: rileva quindi **il comportamento** del contribuente complessivamente considerato e valutato ex post sulla base degli effetti cui ha dato luogo. L'art. 6, comma 5-bis riguarda le conseguenze della **singola violazione**, non il comportamento del

contribuente complessivamente considerato: è necessario che la singola violazione non abbia arrecato concreto pregiudizio all'esercizio delle azioni di controllo, non abbia inciso sulla determinazione della base imponibile e del tributo ed infine non abbia avuto conseguenze ai fini del versamento.

7. La fattura come "contenitore" di dati fiscalmente rilevanti ed il problema degli studi di settore

L'informatizzazione della fattura permette di disporre di uno straordinario strumento per l'elaborazione, rilevante ai fini tributari, di dati ed informazioni relativi alla situazione contabile e finanziaria dell'impresa e dello studio professionale.

Il D.M. tuttavia non sembra cogliere quest'aspetto innovativo: all'art. 3 infatti si dispone che i documenti informatici, rilevanti ai fini tributari, tra l'altro devono consentire la funzione di ricerca e di estrazione delle informazioni, dagli archivi informatici, in relazione al nome, al cognome, alla denominazione, al codice fiscale, alla partita IVA alla data o associazioni logiche di questi ultimi.

Si tratta di un approccio riduttivo perché gli aspetti di pianificazione e di controllo di gestione sono presenti nella realtà imprenditoriale come in quella professionale: in entrambi i casi l'informatizzazione delle scritture contabili consente l'elaborazione dei dati contenuti in fattura secondo le indicazioni del novellato art. 21 D.P.R. 633/1972. L'informatizzazione della contabilità e la sua "smaterializzazione" fanno assurgere alla "contabilità industriale" e, con riferimento agli studi professionali, alla contabilità gestionale piena valenza tributaria ai fini, in particolare, della possibilità di dimostrare la congruità e la coerenza dei componenti positivi e negativi del reddito d'impresa/professionale dichiarati.

Questa riflessione introduce il problema degli "studi di settore" che sono realizzati sulla base dei dati complessivi forniti dai contribuenti, in riposta ad appositi questionari predisposti ed inviati dall'amministrazione finanziaria. La costruzione degli studi è possibile anche grazie alla collaborazione delle associazioni di categoria e degli ordini professionali, che intervengono sia nella fase di elaborazione dello studio che nella fase di revisione e monitoraggio. La Cassazione con la sentenza n. 2891 del 27 febbraio 2002 ha affermato la legittimità dell'accertamento basato sugli studi di settore - considerati elementi presuntivi – e ha dichiarato ammissibile che il contribuente adduca delle prove "a contrario" servendosi a tal fine di altre presunzioni tese a confermare la validità del suo operato. Pertanto la rilevanza, anche a fini tributari, dei documenti contabili informatici e delle scritture ad essi relative comporta la possibilità di elaborare le informazioni della specifica realtà imprenditoriale e professionale ed opporle a quelle desunte dalle metodologie che sono alla base degli studi di settore.

BIGLIOGRAFIA ESSENZIALE

S. Capolupo, Commercio elettronico, fatturazione elettronica e microfilmatura ottica, in Il Fisco, 15/2004

U. Zanini, La fattura elettronica dalla direttiva UE ai nuovi scenari, in http://www.interlex.it 15.04.04

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO
Problematiche
di formazione e probatorie

Email, documento informatico e privacy

Per affrontare la tematica, pur nei ristretti limiti di tempo, è necessario innanzitutto qualificare la natura del diritto alla riservatezza.

Il sistema costituzionale non conosce una norma espressa che appresti tutela al diritto alla riservatezza (al pari della legislazione ordinaria prima dell'introduzione della normativa sulla privacy).

Si pensi che a metà degli anni '50 la Cassazione riteneva non sussistere nel nostro ordinamento un simile diritto (sentenza n. 4487/1956) e che solo a metà degli anni sessanta cominciò ad affacciarsi la tutela di tale diritto (Cass. n. 990/1963).

Bisogna attendere il 27.05.1975 per vedere affermata dalla Suprema Corte l'esistenza di un diritto alla riservatezza nel nostro ordinamento.

Le norme costituzionali citate a sostegno del riconoscimento del diritto in esame sono gli artt. 2 e 3 Cost. In particolare la natura di "norma aperta" dell'art. 2 consentirebbe di riconoscere - come osserva Prosperi - rango costituzionale alla garanzia di sottrarre

all'intrusione di terzi determinate informazioni che se liberamente conosciute non assicurerebbero il pieno godimento dei diritti e delle libertà fondamentali sancite dalla Costituzione.

L'art. 3 viene indicato a sostegno dell'esistenza di questo diritto richiamando la necessità della tutela di una sfera privata inviolabile a garanzia della dignità e dello sviluppo dei diritti della persona.

Alcuni autori hanno poi trovato fondamento costituzionale al diritto alla riservatezza nell'art. 21, che riconosce il diritto di manifestare il proprio pensiero e che pertanto implicherebbe anche la possibilità di non manifestarlo in tutto o in parte, con la conseguenza che tutte le attività finalizzate ad apprendere e diffondere il pensiero che non si vuole manifestare all'esterno lederebbero la libertà garantita dall'art. 21 (il c.d. diritto al silenzio).

Viceversa, gli artt. 13,14,15, e 27, 2° comma, della Costituzione sono stati ritenuti riferimenti parziali e non decisivi per poter affermare l'esistenza a livello costituzionale di un diritto alla riservatezza.

Il variegato richiamo a queste norme ha fatto concludere a Pizzorusso che "il riconoscimento anche a livello costituzionale del diritto alla riservatezza abbia a fondarsi, più che su una od un'altra norma, su un complesso di argomenti interpretativi che consentono di dimostrarne l'esistenza come principio non scritto della Costituzione".

Tale diritto ha avuto riconoscimento tra le norme Comunitarie tramite le Direttive 95/46 CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera

circolazione di tali dati), Direttiva 97/66 CE (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni), nonchè da ultimo dalla Direttiva 2002/58 CE (relativa al trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche).

Di sicuro, la Legge 31.12.1996 n. 675 ha posto all'attenzione dei giuristi l'esistenza non solo di un diritto alla riservatezza, ma altresì di un diritto alla corretta circolazione dei dati personali, da attuarsi anche attraverso il controllo che può essere esercitato sugli stessi da parte dell'interessato.

Il Gruppo Europeo, con specifica Opinion in materia, ha chiarito che il diritto alla privacy non è un diritto assoluto, sebbene sia tra quelli fondamentali e che va bilanciato con altri diritti o interessi legittimi o libertà.

Questo diritto è peraltro destinato per sua natura a contrapporsi ad altri concorrenti diritti esistenti nell'ordinamento.

Limiterò pertanto la mia esposizione alla disamina di alcune situazioni conflittuali che maggiormente si rinvengono nella pratica.

Uno dei conflitti possibili è quello tra privacy e diritto alla difesa.

Con una recente Ordinanza il Tribunale di Santa Maria Capua Vetere, nel decidere un ricorso d'urgenza promosso avverso la produzione in un giudizio di separazione (cui la ricorrente era estranea) di fotografie, che ritraevano la ricorrente e ritenute dalla stessa pregiudizievoli della riservatezza e dell'immagine, ha osservato che le esenzioni di cui agli attuali artt. 13,5° comma e 24 lett. f), nonché

la circostanza che nessuno può accedere alla visione del fascicolo processuale eccetto gli aventi diritto, farebbero venire meno le lamentele della ricorrente sulla violazione del diritto alla riservatezza. Osservava lo stesso Tribunale che nel corso della prova testimoniale (relativa al giudizio di separazione) qualcuno dei testimoni avrebbe comunque potuto citare il nome della parte ricorrente, facendo così venire meno il diritto alla riservatezza. Il Tribunale statuiva quindi il rigetto del ricorso sul presupposto che le finalità della Giustizia sono esigenze di rango superiore che (come riconosciuto dalla stessa normativa sulla privacy) consentono di sacrificare l'altrui diritto alla riservatezza. L'Ordinanza parrebbe peraltro non pienamente condivisibile, quantomeno laddove fa riferimento all'eventualità che un testimone potesse riferire nell'ambito della prova il nome della parte (che ha poi proposto ricorso ex art. 700). Infatti, la circostanza non comporta che quel nominativo dovesse necessariamente entrare nel verbale della causa, ben potendo, proprio per la salvaguardia delle esigenze di riservatezza altrui, ritenersi legittima l'omessa menzione da parte del Giudice del nominativo della persona implicata nella relazione extraconiugale. In altri termini, il fatto che andava provato era l'esistenza della relazione extraconiugale e non la rivelazione di chi (come estraneo al giudizio di separazione) era coinvolto nella stessa.

Inoltre, se è pur vero che l'istruzione probatoria di una causa civile può essere il momento in cui si giustifica la compressione del diritto all'altrui riservatezza, non è altrettanto vero che tale compressione

possa essere estesa a tutti i casi ed a tutti i documenti (scritture private, fotografie o altre prove documentali), senza un attento esame dell'eccedenza di tali produzioni rispetto alle finalità di difesa collegate al diritto fatto valere.

La norma di riferimento per risolvere il conflitto è l'art. 24 Cost., di cui sono corollario le norme del T.U. che prevedono espressamente la non necessarietà del consenso allorquando il trattamento del dato personale sia necessario per far valere o difendere un diritto in sede giudiziaria. Questa esenzione, per quanto riguarda i dati sensibili, deve essere peraltro interpretata e collegata caso per caso con il disposto dell' art. 26 D.Lgs. n. 196/03 sulla privacy.

In particolare, per il trattamento dei dati sensibili, idonei a rivelare lo stato di salute o la vita sessuale, va verificato se gli stessi sono o meno funzionali al riconoscimento in giudizio di un diritto di rango pari a quello alla riservatezza del soggetto cui i predetti dati si riferiscono, oppure se si tratta di far valere un diritto della personalità o un altro diritto fondamentale ed inviolabile. Inoltre, in questa analisi, non si può tralasciare il dettato dell'art. 11 D.Lgs. n. 196/03 in tema di modalità e liceità del trattamento.

Alla luce di quanto sopra detto, va forse rivista la giurisprudenza che riconosce a priori l'esimente della giusta causa di cui al secondo comma dell'art. 616 c.p. (rivelazione del contenuto di corrispondenza) con riferimento, ad esempio, alla produzione in un giudizio di separazione personale di corrispondenza indirizzata al coniuge, produzione nel caso esaminato finalizzata a contrastare una

richiesta di assegno di mantenimento.

In conclusione, si può ritenere che le finalità della Giustizia sono in linea di principio esigenze di rango superiore rispetto al diritto alla riservatezza, non peraltro in senso assoluto, ma con valutazioni da effettuarsi caso per caso.

Sul tema possono trarre in inganno le pronunce, anche recenti, che considerano prevalente il diritto di difesa del lavoratore dipendente (che produca in giudizio documenti aziendali riservati al fine di ottenere il riconoscimento di un proprio diritto) sul diritto di segretezza e riservatezza dell'azienda garantito dal cod. civ.; trattasi infatti di diritto diverso da quello della riservatezza, come configurato dal nuovo T. U. sulla privacy. Riterrei pertanto dette pronunce non significative in relazione al tema trattato.

Un altro possibile conflitto con il diritto alla riservatezza può verificarsi in relazione al diritto di controllo del datore di lavoro sull'uso da parte del dipendente degli strumenti informatici aziendali sia sotto il profilo dell'accesso ad internet per finalità extralavorative che sotto quello dell'abuso della casella postale informatica.

Nessun dubbio sul fatto che il datore di lavoro disponga dei mezzi tecnici per poter effettuare detto controllo, venendo a conoscenza in tal modo dei siti web visitati dal dipendente nonché della corrispondenza e-mail ricevuta ed inviata dallo stesso. Il problema è quello di comprendere se detto controllo sia o meno lecito ed in quali limiti possa eventualmente essere effettuato.

Sotto il profilo della tutela della riservatezza del dipendente (nonché

del rispetto della sua libertà e personalità) viene in rilievo l'art. 15 Cost. (a garanzia della libertà e segretezza della corrispondenza), l'art. 616 c.p. (che sanziona la violazione di corrispondenza), l'art. 4 St. Lav. (in tema di divieti di controlli a distanza sull'attività dei lavoratori) nonché la normativa in materia di privacy di cui al D. Lgs. n. 196/03.

E' importante innanzitutto chiarire quali sono le finalità del potere di controllo del datore di lavoro.

Una prima finalità è stata ravvisata nella tutela del patrimonio aziendale, vale a dire nell'interesse dell'imprenditore di evitare una perdita di tempo lavorato da parte dei dipendenti impegnati in attività extralavorative (collegamento ad internet per uso personale) ed una conseguente diminuzione dell'efficienza dell'azienda. Vengono in rilievo sotto il profilo della tutela del patrimonio aziendale anche esigenze di sicurezza informatica connesse alla necessità di proteggere informazione e dati interni dell'azienda da attacchi esterni di vario genere (ad es. virus o attacchi mirati a carpire segreti aziendali). In assenza di indicazioni, il dipendente stesso potrebbe involontariamente causare danneggiamenti ai sistemi informatici (ad esempio installando programmi nocivi, scaricando allegati sospetti, disattivando le protezioni, comunicando le password). Inoltre, possono essere arrecati danni alla reputazione ed all'immagine dell'azienda attraverso messaggi di contenuto extralavorativo o di dubbio decoro inoltrati dai dipendenti a terzi tramite gli indirizzi e-mail dell'azienda.

Un controllo sul traffico telematico è imposto anche dall'obbligo per l'imprenditore di adottare tutte le misure necessarie a tutelare l'integrità fisica e la personalità morale del dipendente (art. 2087 c.c.). Si pensi al possibile contenuto lesivo della dignità del lavoratore di e-mail indirizzate alla casella di posta elettronica allo stesso assegnata, provenienti per ipotesi anche da altri dipendenti a scopo denigratorio o minatorio.

L'esigenza di effettuare i predetti controlli si giustifica anche in relazione all'interesse dell'imprenditore di prevenire la commissione di illeciti da parte del dipendente tramite l'abuso degli strumenti informatici, illeciti che possono coinvolgere l'azienda in responsabilità civili, penali ed amministrative.

Il datore di lavoro può infatti trovarsi a rispondere civilmente ex art. 2049 c.c. anche se il dipendente ha agito oltre il limite delle proprie mansioni o perfino in violazione di ordini ricevuti.

Tramite lo strumento informatico possono essere del pari commessi dal dipendente vari illeciti:

- violazioni della normativa in materia di diritto d'autore (ad es. scaricando illecitamente file o programmi o duplicando programmi);
- reati comuni (quali ad es. ingiuria, diffamazione ovvero rivelazione di segreti aziendali);
- reati legati alla pedopornografia (L.n. 269/98), per i quali è punito anche chi semplicemente disponga del materiale in questione;
- frode informatica a danno dello Stato o di altro ente pubblico (con

possibile applicazione di sanzioni pecuniarie a carico dell'azienda);

- trattamento di dati in violazione della stessa Legge sulla privacy (di cui risponde il datore di lavoro in quanto titolare del trattamento).

Il controllo degli strumenti informatici è inoltre ricompreso tra le misure di sicurezza che il datore di lavoro è tenuto ad adottare in relazione al cd. Codice della privacy.

Consideriamo ora quali sono i limiti imposti dall'ordinamento ai controlli da parte del datore di lavoro.

Viene in rilievo innanzi tutto l'art. 4 St. Lav. (richiamato dall'art. 114 D.Lgs. n. 196/03) che vieta in modo assoluto l'impiego di strumenti audiovisivi o di altre apparecchiature per finalità di controllo sull'attività lavorativa posta in essere dai dipendenti. Il medesimo articolo, al secondo comma, consente l'utilizzo di impianti o apparecchiature di controllo richiesti da esigenze organizzative, produttive o di sicurezza del lavoro, che comportino indirettamente controlli sull'attività lavorativa del dipendente, solo previo accordo con le R.S.U. o con la Commissione interna. Tra gli strumenti di controllo indicati dalla norma si può ritenere che rientri anche l'utilizzo dello strumento informatico, che attua un controllo "occulto" (che può cioè essere effettuato all'insaputa del lavoratore).

Da segnalare una recente pronuncia della Suprema Corte che ha ritenuto consentiti i controlli posti in essere per rilevare eventuali comportamenti illeciti attuati dai dipendenti, ad esempio sistemi di controllo dell'accesso ad aree riservate ovvero apparecchi di

rilevazione di telefonate ingiustificate (Cass. n. 4746/02).

E' stato peraltro precisato che le prove di comportamenti illeciti di dipendenti, ricavate tramite sistemi ed apparecchiature non autorizzate secondo quanto previsto dall'art. 4 St . Lav., non avrebbero validità probatoria in sede processuale e non potrebbero pertanto essere poste a base di provvedimenti disciplinari nei confronti dei lavoratori (Cass. n. 8250/00).

I controlli effettuati tramite gli strumenti informatici vanno pertanto quanto meno previamente autorizzati dagli organismi competenti. Atteso che tramite detti controlli si potrebbero conoscere dati sensibili del dipendente (ad es. rilevando la tipologia dei siti internet visitati), vi è il rischio di violare la disposizione di cui all'art. 8 St. Lav. (che vieta indagini anche indirette su opinioni politiche, sindacali, religiose o altri fatti che esulano dalla vita professionale) nonchè le disposizioni in tema di privacy, che tutelano la vita privata anche nell'ambito del rapporto di lavoro.

Va precisato che il monitoraggio delle e-mail dei lavoratori e degli accessi ad internet costituisce un trattamento di dati personali (newsletter del Garante 17.09.01).

E' pertanto necessario che di tali controlli (che comportano trattamento di dati) sia previamente data idonea informativa ai dipendenti (spiegandone le finalità e le modalità di attuazione). Non sarebbe invece necessario il consenso dei lavoratori in relazione alle esenzioni previste dagli art. 24 lett. a) e 26, 4° comma lett. d), purchè il controllo sia limitato alle operazioni necessarie e pertinenti

alle finalità per le quali è posto in essere.

Un problema connesso è quello della possibile violazione da parte del datore dell'art. 616 c.p. sulla violazione di corrispondenza, nella quale è ricompresa quella informatica. Si segnala che l'Autorità Garante qualifica la e-mail come corrispondenza chiusa. E' stato peraltro osservato che la casella postale aziendale è di proprietà e pertinenza dell'azienda che ne concede l'utilizzo al dipendente per lo svolgimento dell'attività lavorativa. Si è ritenuto pertanto che non violi l'art. 616 c.p. il datore di lavoro che, all'insaputa del lavoratore, controlla la sua posta elettronica sulla casella aziendale, atteso che il lavoratore non è titolare di un diritto all'utilizzo esclusivo della posta elettronica aziendale (Trib. Milano 10.05.02).

Il Garante, inoltre, considera lecito un controllo delle e-mail solo in casi eccezionali, come per la rilevazione di virus o per prevenire attività criminose del dipendente ovvero in assenza o impedimento del lavoratore.

Sarebbe consigliabile pertanto regolamentare a priori l'accesso e l'utilizzo del sistema di posta elettronica dell'azienda limitando l'uso della stessa da parte del dipendente per le sole finalità lavorative ovvero tramite l'indicazione di regole che il dipendente deve osservare per un utilizzo per motivi extralavorativi.

Il Gruppo europeo per la protezione dei dati (organismo della Comunità istituito in base all'art. 29 della direttiva 95/46/EC) ha dato alcune indicazioni e suggerimenti per il tema che ci interessa tra i quali quello di consentire l'accesso ad internet ai soli lavoratori che

necessitano di tale connessione, dotare di una casella e-mail aziendale (del tipo nomecognome@nomeazienda.it) solo i lavoratori che devono tenere contatti con l'esterno o con altri dipendenti dell'azienda, dotarsi di strumenti (proxyfirewall) che impediscono l'accesso alla rete in orario extralavorativo, bloccare il collegamento a categorie predeterminate di siti web ovvero consentire la connessione solo ad una lista di siti autorizzati, configurare il server in modo da impedire l'acceso ad e-mail con allegati sospetti.

E' infatti preferibile, sotto il profilo della legittimità del comportamento tenuto dal datore, che lo stesso si cauteli inibendo a monte l'accesso a determinati siti (ed agendo pertanto in via preventiva) piuttosto che essere costretto ad intervenire con controlli successivi che facilmente comportano il trattamento di dati personali e che, per di più, possono essere inidonei a rimuovere eventuali effetti dannosi già prodotti.

Ricordiamo infine che è contemplata dalla Legge sulla privacy la possibile adozione di un codice deontologico che regolamenti il trattamento dei dati personali nell'ambito del rapporto di lavoro (art. 111), ed è auspicabile che detto codice disciplini compiutamente le problematiche di controllo sovraesposte.

Una ulteriore ipotesi di conflitto può verificarsi tra diritto alla riservatezza e diritto di accesso che un terzo intenda esercitare su documenti amministrativi contenenti dati personali.

Nello specifico, l'art.59 del cd. Codice sulla privacy prevede sia per i dati personali in genere che per quelli sensibili e giudiziari che il

diritto di accesso trovi la sua disciplina nella L. n. 241/90 e successive modifiche e nelle altre leggi in materia e relativi regolamenti di attuazione. Sostanzialmente per i dati personali sensibili e non, il legislatore nulla ha innovato rispetto all'indirizzo giurisprudenziale portato dalla fondamentale, ed ancora attuale, pronuncia del Consiglio di Stato in Adunanza Plenaria nr.5/97, che riconosceva la cosiddetta tutela modale e cioè che il diritto di accesso (avente ad oggetto informazioni relative alla vita privata di un soggetto diverso dal richiedente) in linea di principio soccombe di fronte a quello alla riservatezza ma che, nel caso in cui il diritto di accesso venga esercitato per la cura o difesa di interessi giuridici, detto diritto può essere esercitato peraltro nella sola forma della presa visione.

L'unica eccezione alla scelta della cd tutela modale a favore della valutazione comparativa in concreto tra esigenze contrapposte è prevista nell'art.60, che presenta una particolare tutela per i cd dati super sensibili: i dati relativi alla vita sessuale ed alla salute non sono visionabili se non quando il richiedente con la istanza di accesso vuole tutelare un interesse almeno di pari rango ed egualmente meritevole di tutela.

Riassumendo, la tutela dei dati personali resta assoluta nei confronti di chi chiede un accesso meramente conoscitivo. Se invece il diritto di accesso viene esercitato per difendere o curare propri interessi giuridici, il diritto alla riservatezza soccombe, ma l'accesso è consentito solo nei termini di cui alla Sentenza nr. 5/97. Se, infine,

l'accesso riguarda dati personali sensibili sulla salute o sulla vita sessuale, viene riconosciuta una tutela assoluta al dato, salvo che il richiedente non sia portatore di un interesse di rango pari ed egualmente meritevole di tutela.

Concluderei osservando che il diritto alla riservatezza non è pertanto un diritto assoluto, pur essendo un diritto fondamentale dell'individuo, che peraltro vive ed opera nella collettività. Le relazioni e gli ambiti nei quali si esplica l'esistenza di ogni persona implicano che detto diritto venga a confrontarsi o a scontrarsi con altri diritti ed esigenze. La prevalenza del diritto alla riservatezza o invece di altri diritti va peraltro esaminata e valutata con riferimento alle concrete fattispecie, essendo difficile trovare soluzioni a priori.

Per i dati sensibili relativi allo stato di salute o alla vita sessuale – come visto – è la stessa legge sulla privacy che ne subordina il trattamento all'esigenza di far valere diritti di rango almeno pari ovvero consistenti in un diritto della personalità o altro diritto o libertà fondamentali e inviolabili.

Vi sono pertanto situazioni nelle quali il diritto alla riservatezza può subire limitazioni se inteso come diritto di esclusione degli altri dalla propria sfera personale ma restando comunque sempre tutelato come diritto al corretto trattamento dei dati personali, e quindi nella concreta disamina, da farsi caso per caso, non può prescindersi dall'ulteriore analisi della esattezza, dell'aggiornamento del dato, della completezza e soprattutto della necessarietà, pertinenza e non eccedenza rispetto alle finalità in relazione alle quali viene a poter

essere trattato (Art. 11 D.Lgs. nr. 196/2003)

Grazie dell'attenzione

Avv. Giulia Ferrarese

Bibliografia:

Massimo Prosperi "Il diritto alla riservatezza nell'ordinamento professionale"; Alfonso di Nuzzo "Privacy e diritto alla difesa"; dott. Marco Secco "Il controllo del traffico telematico in azienda"; avv. Andrea Stanchi "Privacy, rapporto di lavoro, monitoraggio degli accessi a Internet, monitoraggio delle e-mail e normative di tutela contro il controllo a distanza."; dott.ssa Azzurra Fodra "Bilanciamento tra diritto di accesso e diritto alla riservatezza: evoluzione normativa e giurisprudenziale in materia".

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO

Problematiche

di formazione e probatorie

Prima di esaminare il tema oggetto della presente relazione, occorrerà fare alcune brevissime puntualizzazioni, atteso che le espressioni "firma elettronica" (meglio: "firme elettroniche") e "firma digitale" non sono sinonimi e la differenza non è solo terminologica.

Quando si parla di **firma elettronica** s'impiega un'espressione di carattere generale, posto che esistono molti tipi di firma elettronica, tutte sostanzialmente tesi ad attribuire ad un messaggio digitale le funzioni proprie della sottoscrizione autografa.

I vari tipi potranno essere distinti per esempio in base al metodo utilizzato: tra i metodi d'autenticazione delle firme ricordiamo quelli legati ad una conoscenza propria dell'utilizzatore (numero di codice), alle sue caratteristiche fisiche (l'impronta della retina), al possesso di un oggetto (tessera magnetica).

In ogni caso, l'art. 1 del DPR n. 445\2000 co I lett. "cc", come modificato dall'art. 2 del DLGS 10\2002, qualifica come tale "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo d'autenticazione informatica".

Si parlerà poi di **"firma elettronica avanzata"** quando questa è "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" (v. art. 1 cit., co. I lett. "dd").

La **firma digitale** è invece una particolare specie di firma elettronica, quella che utilizza il sistema di crittografia a chiave pubblica o asimmetrica (v. art. 1 co. I lett. "n" DPR n. 445\2000 – come modificato dall'art. 2 Dlgs 10\2002: "firma digitale è un particolare tipo di firma elettronica qualificata, basata su di un sistema di chiavi asimmetriche a coppia, una pubblica ed 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…").

Altro concetto fondamentale è quello del **certificatore**, definito dall'art. 1 DPR cit. come il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. Si noti che oggi, dopo la direttiva europea 1999\93\CE ed il recepimento della stessa nel nostro ordinamento ad opera del Dlgs. n. 10\2002 (v. oltre), l'attività di certificazione è libera e non necessita d'autorizzazione preventiva, così innovandosi rispetto al rigoroso sistema delineato dal legislatore italiano con i DPR n. 513\1997 e 445\2000, che prevedevano un unico certificato normativamente disciplinato e un'unica figura di certificatore, inserita in un apposito elenco pubblico dopo aver dimostrato di possedere vari requisiti tecnici, giuridici e morali (v. art. 27 DPR n. 445\2000).

I **certificati elettronici** sono, sempre secondo la stessa disposizione di legge, gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (nell'art. 1 in esame si possono poi individuare vari tipi di certificato e di certificatori, cui si può fare integrale rinvio).

Passando al tema che ci occupa, il riferimento normativo principale è costituito dall'**art. 10 DPR 445\2000**, come novellato dall'art. 6 DLGS 10\2002.

Tale norma è stata come sopra modificata per adeguare l'ordinamento italiano alla direttiva n. 1999\93\CE del Parlamento Europeo e del Consiglio.

Con tale direttiva, come s'è visto, si voleva liberalizzare il mercato dei certificatori e la circolazione delle firme elettroniche e, pertanto, si è reso necessario operare con la citata novella.

Il **I comma dell'art. 10 cit.** prevede che "il documento informatico ha l'efficacia probatoria prevista dall'art. 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate".

Con l'ultimo inciso, quindi, si riporta la medesima formulazione utilizzata dal CC, con l'ovvia, ulteriore aggiunta che tale efficacia è subordinata al fatto che "colui contro il quale" il documento è prodotto "non ne disconosce la conformità ai fatti o alle cose medesime" (occorrerà pertanto, secondo la costante giurisprudenza di legittimità – v. p.es., Cass. Civ., 3.7.2001 n. 8998 – una contestazione esplicita, processualmente equiparabile ad un'ordinaria eccezione in senso lato, e in tal caso il giudice potrà accertare la contestata conformità con ogni mezzo di prova, ivi incluse le presunzioni – v. Cass. Civ., 6.9.2001 n. 11445).

Ovviamente, il documento informatico di cui sopra è un documento non sottoscritto né digitalmente né in altra maniera. Come tale, ci si rende conto che la norma in esame si applicherà alla gran parte dei

documenti che transitano nella rete (diverso è il caso, affrontato dalla recente Cass. Civ. Sez. Lavoro, 16.2.2004 n. 2912, che ha ritenuto non utilizzabile a fini probatori una copia di "pagina Web" trasferita su supporto cartaceo, che non risulti esser stata raccolta con garanzia di rispondenza all'originale e di riferibilità ad un ben individuato momento).

In ogni caso, nulla dice il legislatore circa l'integrità del documento, anche se spesso ciò che è importante accertare non è la paternità, ma l'assenza di modifiche o falsificazioni. Benché probabilmente ci sia la possibilità tecnica di delineare vari livelli di sicurezza, in assenza di disposizioni specifiche, tale possibilità potrà esser prospettata dalla parte che intende avvalersi del documento al giudice, onde contribuire a formare il suo libero apprezzamento della prova, fermo restando che ogni difesa di controparte dovrà comunque basarsi sul citato disconoscimento.

Nella attesa del cd. processo informatico, il problema pratico è quello della consultabilità di siffatto documento: perché non sia altrimenti sempre necessario un "computer" occorrerà trasferire il suo contenuto su carta. Onde risolvere tale problema, il giudice potrà disporre nei casi più semplici (sostanzialmente risolventisi in una trascrizione) la riproduzione ex art. 261 CPC del documento informatico su carta, mentre, per i casi più complessi (si pensi a

documenti danneggiati o parzialmente crittografati), si potrà ricorrere ad una CTU e\o all'ispezione di cui all'art. 259 CPC (a quest'ultimo istituto si dovrà ricorrere, con o senza l'assistenza del CTU, quando il contenuto del documento non sia riproducibile su carta – si pensi a brani musicali o a sequenze filmate).

Passando al **II comma dell'art. 10 cit.,** con esso si stabilisce che "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".

Per un attimo richiamando quanto sopra detto in tema di firma elettronica, la norma in esame non attribuisce al documento in esame una precisa efficacia probatoria: non avremo quindi una prova legale, ma una prova soggetta alla libera valutazione del giudice ex art. 116 CPC. Il "peso" probatorio di tale documento non sarà percepibile prima del processo, ma diverrà evidente solo in esito alla suddetta valutazione e, quindi, al processo.

L'incertezza aumenta sol che si consideri la citata genericità definitoria del legislatore in tema di firma elettronica e la

conseguente possibilità di configurare svariati tipi di tale firma (più sicuri o meno sicuri a seconda del tipo d'autenticazione prescelto). Proprio per tali motivi appare del tutto condivisibile la scelta di affidare al giudice la decisione da adottare caso per caso: con la norma in questione, peraltro, si è definitivamente e pienamente legalizzato l'uso di siffatte prove, così per esempio potendosi provare una transazione economica attraverso la traccia elettronica della carta di credito. Del resto, così facendo si è data piena attuazione alla direttiva europea 1999\93\CE che prevedeva per gli stati membri l'impossibilità di considerare inammissibile o inefficace la firma elettronica per il solo fatto della sua "elettronicità" o dell'assenza di una sua certificazione o creazione in termini di sicurezza.
Bisogna comunque rilevare che la prova in esame non è considerata come scrittura privata ex art. 2702 CC, pur soddisfacendo "il requisito legale della prova scritta". Ne conseguirà che gli atti o i contratti per la cui validità si richiede la forma scritta potranno esser contenuti nei documenti informatici con firma elettronica, ma la loro efficacia probatoria non sarà quella della scrittura privata, rimanendo affidata al giudice ex art. 116 CPC. Ancora una volta, però, attesa la possibilità di adottare legittimamente svariati tipi di firma elettronica, la altrimenti poco comprensibile separazione tra validità ed efficacia probatoria del documento con firma elettronica appare comunque

giustificata, altrimenti potendosi attribuire, in nome di formali esigenze concettuali, la medesima, rilevante efficacia probatoria a più o meno sicuri metodi d'autenticazione.

Più complesso è il successivo **comma III dell'art. 10 cit.**.

In esso si parla di "firma digitale", di "firma elettronica avanzata", di "certificato qualificato", di un "dispositivo per la creazione di una firma sicura" (per la nozione relativa a queste due ultime definizioni, v. art. 1 co. I lett. "aa" e "ii" DPR n. 445\2000).

Si delineano pertanto due tipi di documento informatico (uno sottoscritto con firma digitale ed uno sottoscritto con l'utilizzo degli altri tre strumenti sopra elencati), ambedue peraltro dotati dell'efficacia di piena prova, fino a querela di falso (verosimilmente, l'oggetto di tale giudizio si incentrerà in genere sull'uso abusivo o illecito di una chiave privata altrui). L'efficacia sarà pertanto quella della scrittura privata riconosciuta o non disconosciuta ex art. 2702 CC.

Quanto alla **firma digitale**, essa era già conosciuta dall'ordinamento previgente (v. DPR n. 513\1997 e 445\2000 ante novella), ma la norma in esame ha il pregio di dirimere una controversia sorta per l'appunto in tale periodo: ferma restando per documento sottoscritto con la firma digitale l'efficacia di cui all'art. 2702 CC, si discuteva in dottrina se tale efficacia fosse già in prima battuta fino a querela di

falso o se, invece, per arrivare a tale risultato si dovesse autenticare la sottoscrizione o la si dovesse riconoscere o non disconoscere.
Oggi, pertanto, tale tipo di documento non potrà più esser disconosciuto ex art. 215 CPC, ma potrà esser solamente impugnato con la querela di falso.
Sotto un profilo tecnico, il dispositivo di autenticazione a chiavi asimmetriche riesce a garantire non solo la provenienza della dichiarazione informatica, ma anche l'integrità del documento che la contiene, perché, se si modifica un suo elemento anche minimo dopo la cifratura con la chiave privata, tale documento non viene più riconosciuto dalla chiave pubblica nell'ambito della procedura di verifica.
Sempre in tema di firma digitale, ci si chiede come coordinare il parimenti vigente disposto del successivo art. 24 ("si ha per riconosciuta, ai sensi dell'art. 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato") con la disposizione in esame, che considera la firma digitale già munita, in sé e per sé, dell'efficacia di prova legale.
Secondo una parte della dottrina si sarebbe verificata un'abrogazione tacita dell'art. 24 da parte dell'art. 6 DLGS 10\2002 (che ha per l'appunto modificato l'art. 10 in esame), mentre secondo altri le due

norme possono ancora coesistere (infatti, in caso di firma autenticata – art. 24 - l'oggetto della querela di falso verterà unicamente sulla falsità della dichiarazione del pubblico ufficiale, avendo quest'ultimo certificato la coincidenza tra utilizzatore e titolare della chiave privata; nei restanti casi – art. 10 -, tale oggetto verterà sull'abusivo o fraudolento uso della chiave privata).

Quanto alla **firma elettronica avanzata**, il livello e lo "standard" di sicurezza da cui derivano l'efficacia probatoria privilegiata del documento non sono individuati con precisione dal punto di vista tecnico, limitandosi il legislatore a prevedere tre requisiti minimi necessari per la sicurezza delle firme elettroniche, con chiari utilizzo e attuazione del principio di "neutralità tecnologica", a cui si è sempre ispirata la legislazione comunitaria.

Ovviamente, a tale ampia e pragmatica apertura tecnologica (verosimilmente ispirata da criteri economici e imprenditoriali propri di un regime di libera concorrenza e di libero mercato), dovrà fare da contraltare (anche alla luce della rilevantissima efficacia probatoria attribuita al documento in esame) un quanto mai rigoroso e severo controllo su quel terzo che contribuisce a garantire, attraverso il rilascio del certificato qualificato, l'autenticità della sottoscrizione, a pena di rendere meno sicuri i traffici commerciali e la circolazione dei beni (v. artt. 26, 27 e 29 DPR 445\2000 testo vigente).

Anche per la firma elettronica avanzata, come per la firma digitale, la garanzia di autenticità dovrebbe valere sia per la provenienza che per l'integrità del documento, altrimenti nessun senso avendo l'inciso contenuto nella norma definitoria di cui all'art. 1 co I lett. "dd" già citato ("… consentire di rilevare se i dati stessi siano stati successivamente modificati").

Abbiamo quindi visto che i due tipi di sottoscrizione esaminati nel comma III garantiscono tanto la provenienza quanto l'integrità del documento informatico, epperò la "piena prova, fino a querela di falso" è in esso limitata alla sola "provenienza delle dichiarazioni di chi l'ha sottoscritto".

Orbene, attesa la non contestabilità di quanto prima rilevato sotto l'aspetto tecnico dei due tipi di firma, appare possibile interpretare estensivamente la disposizione in questione, nel senso di poter estendere la suddetta efficacia probatoria anche all'integrità del documento.

La validità della certificazione apposta sia in caso di firma digitale che in caso di firma elettronica avanzata, peraltro, avrà un termine di scadenza stabilito dal certificatore (v. art. 4 co. VII allegato tecnico al DPCM 8.2.1999 – il termine massimo, stabilito in tre anni dall'art. 22 co I lett. "f" del DPR 445\2000, non esiste più, a seguito della modifica operata dall'art. 8 DPR 7.4.2003 n. 137).

Non resta che esaminare il **IV comma dell'art. 10 cit.**.

Il testo di tale norma, in sostanza riproducente il dettato dell'art. 5 co. II della direttiva europea, comporta due conseguenze.

La prima, secondo cui inevitabilmente deve riconoscersi dignità di prova ai documenti informatici ivi descritti, fermo restando che gli stessi dovranno esser valutati dal giudice ex art. 116 CPC e potranno esser disconosciuti dalla controparte secondo le vigenti regole procedurali ex artt. 214 e ss CPC, con il conseguente, eventuale innesto, nella causa in corso, del procedimento di verificazione ex art. 216 CPC.

La seconda, in base alla quale si può ipotizzare la presenza e la diffusione di sistemi di certificazione e di sottoscrizioni privi dell'efficacia privilegiata propria delle firme di cui ai precedenti commi, ma purtuttavia legittimi e qualificati, sia pure nei limiti già visti, come prove.

Rimane da comprendere l'utilità di siffatta norma, apparendo la stessa assorbita e ricompresa nel più ampio disposto del primo e del secondo dell'art. 10 (le differenze – esigue per la verità - sembrano consistere nel fatto che nel primo comma ci si muove nell'ambito dell'efficacia probatoria propria dell'art. 2712 CC, nel secondo e nel quarto nell'ambito dell'efficacia propria degli artt. 116 e 214 e ss CPC, evidenziandosi peraltro che nel secondo non v'è un

certificatore, mentre nel quarto c'è un certificatore privo degli attributi previsti dalla legge per ottenere l'efficacia della piena prova).

Per concludere, qualche brevissima considerazione sulla **data del documento informatico,** atteso che in tale materia è immediatamente percepibile la novità delle norme in tema di documento informatico rispetto a quella contenuta nell'art. 2704 CC. L'art. 14 co II del DPR 445\2000 prevede, infatti, che "la data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico ed alle regole tecniche di cui agli articoli 8, comma 2, e 9, comma 4, sono opponibili ai terzi".

L'attribuzione della data avviene attraverso la cd. procedura di validazione, definita dall'art. 22 lett. "g" del DPR 445\2000 come "il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi": si tratta in sostanza di una dichiarazione proveniente da un certificatore (ente abilitato a fornire un servizio di validazione temporale) chiamata "marca temporale", modellata secondo il già noto sistema delle chiavi asimmetriche.

Il documento, quindi, conterrà la sottoscrizione di chi ha apposto la marca temporale (tale strumento tecnico è fra l'altro congegnato in

modo tale da non consentire al certificatore di conoscere il contenuto del documento), sottoscrizione che si potrà aggiungere a quella di chi ha certificato la firma digitale.

Anche la validità di tale certificazione temporale, peraltro, avrà il termine di scadenza stabilito dal certificatore (v. art. 4 co. VII allegato tecnico al DPCM 8.2.1999, già sopra citato).

Orbene, per prolungare la suddetta validità o, meglio efficacia probatoria (e quanto si dirà vale anche per le certificazioni in tema di firma digitale ed elettronica avanzata), in base allo schema regolamentare previsto dall'art. 60 dell'allegato tecnico al DPCM cit., l'interessato dovrà, prima della scadenza, procedere alla (nuova) validazione temporale del documento il cui certificato di firma digitale stia scadendo (si prorogherà così la sua efficacia privilegiata per un periodo uguale a quello della validazione temporale effettuata, salvo nuovi, successivi rinnovi) o ottenere una nuova marca temporale prima della scadenza di quella già esistente (la data del documento continuerà così ad esser opponibile ai terzi): ovviamente, potendo coesistere sul medesimo documento i due tipi di certificazione, il rinnovo aggiornerà l'efficacia probatoria del documento sotto il duplice profilo certificatorio.

La parte dovrà quindi preoccuparsi di tener d'occhio le scadenze dei termini fissati dal certificatore, in caso contrario residuando pel

documento l’efficacia probatoria prevista, a seconda dei casi, dai commi I, II o IV dell’art. 10 DPR 445\2000.

Verona, 7.5.2004.

(dott. Ernesto D’Amico)

Giudice del Tribunale di Verona

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO
Problematiche
di formazione e probatorie

Azioni di disconoscimento del documento informatico

Avv. Marisa Bonanno – foro di Verona*

Il documento, quale rappresentazione di una realtà, assolve da una parte alla funzione sostanziale di conferire riconoscimento giuridico ad un atto, dall'altra alla funzione probatoria, nel caso concreto, dell'imputabilità di una certa manifestazione al suo autore o della conformità di una certa riproduzione alla realtà originale. Inoltre il documento rappresenta anche la forma, cioè il modo di trasmissione di una certa volontà.

La disciplina codicistica della prove documentali è volta ad evidenziare validi criteri di riconoscimento di efficacia probatoria al modo di manifestazione di una rappresentazione, che prima dell'avvento del documento informatico si esprimeva attraverso segni grafici.

Secondo il nostro sistema giuridico, l'imputabilità di una rappresentazione ad un soggetto è garantita (con eccezione del testamento olografo, in cui si richiede l'autografia dell'intero documento) dalla **sottoscrizione**; in virtù dell'autenticazione a opera del notaio ovvero del mancato disconoscimento o della verificazione, tale imputabilità costituisce "piena prova" nel processo.

L'ordinamento non prevede tuttavia alcuna regolamentazione della "sottoscrizione". Fra le funzioni assolte dalla sottoscrizione, al fine di garantire la sicurezza e l'autenticità del documento, la dottrina ha evidenziato quelle: indicativa dell'identità del mittente, dichiarativa della paternità del contenuto, probatoria del contenuto stesso; i requisiti della sottoscrizione sono stati individuati nell'autografia, nella nominatività, nell'inequivocabilità e non riproducibilità.

In questo quadro, il documento informatico e la "firma" del medesimo si pongono come "evoluzione biologica" del documento cartaceo, prefiggendosi il legislatore di sopperire con regole tecniche alla difficoltà di riconoscere alla sottoscrizione informatica le stesse garanzie offerte dalla sottoscrizione manuale, ai fini dell'imputabilità della dichiarazione, e di coordinare la disciplina codicistica vigente sulle prove documentali e relative procedure di acquisizione con le peculiarità dei nuovi strumenti.

Con riferimento precipuo alle problematiche probatorie ed in particolare alle diverse forme, per lo più di creazione giurisprudenziale, di azioni ed eccezioni di "disconoscimento" processuale (in senso lato), analizziamo quindi le diverse tipologie di documenti informatici previsti dal vigente DPR n.445/2000, come modificato dal d.lgt. 23 gennaio 2002, n. 10 e relativo regolamento di coordinamento DPR n.137/2003:

a) documento informatico non sottoscritto, cui è riconosciuta - quanto ai fatti e alle cose rappresentate – *"l'efficacia probatoria prevista dall'art. 2712 del codice civile"*, al pari dunque delle riproduzioni meccaniche (art.10 comma 1 DPR 445/2000 modif.).
In questa ipotesi non si tratta di dimostrare l'imputabilità del documento, essendo privo di sottoscrizione, bensì di stabilire quali siano stati gli strumenti utilizzati per la formazione di quella rappresentazione informatica spostando il fulcro dell'accertamento giudiziale sul versante dell'**attendibilità** della riproduzione.

La parte contro cui il documento informatico venga utilizzato avrà quindi l'onere, per evitarne la piena efficacia probatoria, di contestarne la conformità ai fatti o alle cose rappresentate. Sarà allora la parte che intenda utilizzare la riproduzione informatica a dover assolvere l'onere probatorio a suo carico anche dimostrando l'idoneità dello strumento a fornire una **corretta rappresentazione della realtà** e una **sicura riproduzione dei dati**.

Secondo la giurisprudenza della Cassazione: "L'efficacia probatoria delle riproduzioni meccaniche è subordinata - in ragione della loro formazione al di fuori del processo - al mancato disconoscimento ad opera della parte contro la quale sono prodotte in giudizio; tale disconoscimento pur se non è soggetto ai limiti temporali ed alle modalità di cui allo art. 214 c.p.c., deve tuttavia essere **chiaro, circostanziato ed esplicito, dovendo concretizzarsi nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta, e deve avvenire nella prima udienza o nella prima risposta successiva alla rituale acquisizione delle riproduzioni** (nella specie, la SC ha escluso la validità del disconoscimento di una cassetta videoregistrata, stante la condotta processuale della parte la quale, dopo aver assistito alla relativa visione senza muovere alcuna contestazione sui fatti e sui soggetti in essa rappresentati, ne aveva poi genericamente disconosciuto il contenuto in corso di causa, dopo l'esaurimento del termine a tal fine concesso dal giudice)" *Cass., sez. lav., 3 luglio 2001, n. 8998, in Foro it., 2002, I, 2793, n. IOZZO.*

Nell'interpretazione della disposizione che ci occupa è fondamentale la sentenza n. n.11445/2001, con cui la SC, interpretando il comma 2 del previgente art.5 DPR 513/97 in senso conforme alla norma oggi vigente soprarichiamata, ha chiarito che il **disconoscimento** della conformità di una delle riproduzioni menzionate nell'art. 2712 cod. civ. ai fatti rappresentati non ha gli stessi effetti del disconoscimento previsto dall'art. 215, comma secondo, cod. proc. civ., della scrittura privata, perché, mentre quest'ultimo, in mancanza di richiesta di verificazione e di esito positivo di questa, **preclude l'utilizzazione della scrittura, il primo non impedisce che il giudice possa accertare la conformità all'originale anche attraverso altri mezzi di prova, comprese le presunzioni** *(in questo senso anche: Cass. 12 maggio 2000 n. 6090, in tema di copie fotostatiche; Cass. 26 gennaio 2000 n. 866 e Cass. 5 febbraio 1996 n. 940, in tema di copie fotografiche, Cass. 22 dicembre 1997 n. 12949 in tema di tabulati informatici riepilogativi di retribuzioni, Cass. 8 luglio 1994 n. 6437 in tema di dischi cronotachigrafi; Cass. 10 settembre 1997 n. 8901 sugli oneri probatori dell'utente che contesti la corrispondenza al proprio traffico telefonico delle risultanze del misuratore di centrale).*
In particolare la Corte, nel richiamarsi ad altre precedenti decisioni affermative della legittimità del licenziamento disciplinare di lavoratori dipendenti, che presupponevano, in maniera espressa o implicita, la questione della valenza probatoria di sistemi informatici *(Cass. 24 maggio 1999 n. 5042 e Cass. 11 febbraio 2000 n. 1558, relative ad esattori della società Autostrade, per inadempienze accertate con le registrazioni informatiche; Cass. 20 gennaio 1998 n. 476, in tema di inadempienze di dipendente bancario risultanti dal*

sistema informatico) formulava il principio di diritto secondo cui: "in tema di licenziamento per giusta causa, i dati forniti da un sistema computerizzato di rilevazione e documentazione possono costituire, ai sensi dell'art. 2712 cod.civ., e dell'art. 5, comma 2; D.P.R. 10 novembre 1997, n. 513, prova del fatto contestato, **ove sia accertata la funzionalità del sistema informatico e le risultanze di esso possano assurgere a prova presuntiva congiuntamente a circostanze esterne ad esso, altrimenti provate**." Si precisava tra l'altro che le norme del codice civile sul disconoscimento della conformità all'originale di **copie fotostatiche non autenticate** di una scrittura (art.2719) si applicano solo quando questa sia fatta valere come negozio per derivarne direttamente e immediatamente obblighi, e non anche quando il documento sia esibito al solo fine di dimostrare **un fatto storico** da valutare nell'apprezzamento di una più complessa fattispecie, restando in tal caso il giudice libero di formarsi il proprio convincimento utilizzando qualsiasi circostanza atta a rendere verosimile un determinato assunto, come qualsiasi altro indizio, purché essa appaia grave, precisa e concordante *(v. anche Cass. 25.1.1999 n. 659).*

La dottrina ha criticato la decisione per diversi ordini di motivi: a) interpretazione letterale forzata del previgente art.5 DPR 513/97 (argomento oggi superato dalla riforma); b) apparente esclusione dell'utilizzo di CTU; c) conclusione di insufficienza probatoria delle sole risultanze documentali informatiche.

In tema di riproduzioni è da segnalare infine una recentissima sentenza della Cassazione *(n.2912 dell'11 marzo 2004)*, secondo cui va esclusa la qualità di documento (rectius: di prova documentale) in una **copia di pagina web "stampata" su supporto cartaceo** che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento. In questo caso, ci pare di dovere osservare, è la stessa qualità di "riproduzione" ad essere giudizialmente esclusa dalla mera "stampa" del documento informatico, mentre la natura "documentale" della pagina web in sé non può essere messa in discussione come ogni altra rappresentazione grafica.

Per concludere: la Cassazione sostanzialmente riafferma la piena e libera valutazione giudiziale della prova documentale informatica, qualora validamente disconosciuta ai sensi dell'art. 2712, mentre deve aversi per fatto non contestato in caso di mancato disconoscimento.
Osserviamo dunque che nel caso del documento informatico non sottoscritto, l'affidabilità riposta dall'ordinamento appare addirittura maggiore di quanto risulta per un qualunque documento cartaceo non sottoscritto, per il quale non è invocabile, di per sé solo, alcuna efficacia probatoria; ciò evidentemente è da imputarsi alle migliori garanzie, offerte dal primo, quanto meno sotto il solo profilo dell'accertabilità tecnica.

b) documento informatico, sottoscritto con firma elettronica, il quale *"soddisfa il requisito legale della forma scritta" e "l'obbligo previsto dagli artt. 2214 e seguenti del codice civile*" e che, quanto all'**efficacia probatoria**, *"è liberamente valutabile, tenuto conto delle sue caratteristiche di qualità e sicurezza"*; la normativa indica quindi **la rilevanza sostanziale del documento**, precisando anche che ad esso *"non può essere negata rilevanza giuridica, né ammissibilità come mezzo di prova"*. (art.10 comma 2 DPR 445/2000).

L'accertamento giudiziale in questione avrà per oggetto sia la provenienza della dichiarazione che il suo contenuto, rimesso quest'ultimo al principio della libera valutazione (art. 116 c.p.c.) e quindi privo della più forte e (quasi) incontestabile valenza di

"piena prova" della scrittura privata riconosciuta e/o autenticata, assegnato come vedremo alla firma digitale (ed elettronica avanzata).

Il documento informatico sottoscritto con firma elettronica leggera rappresenta, paradossalmente, lo strumento probatorio attualmente più discusso in dottrina; anche perché su questa figura giuridica si innesta l'acceso dibattito dottrinale sul valore probatorio del messaggio e-mail che ha visto protagonista il decreto ingiuntivo n.848/03 del Tribunale di Cuneo.

Nulla dice il legislatore sulle modalità ed effetti dell'eventuale **disconoscimento processuale** (inteso questa volta nel senso sia contenutistico che di attribuibilità al preteso autore). Certo è che **l'esibizione di tale documento informatico comporterà l'accertamento giudiziale della sua autenticità e data di redazione, eventualmente a mezzo di CTU, con valutazione giudiziale diretta delle caratteristiche oggettive di qualità e sicurezza**; il che deve farci ritenere che l'eventuale disconoscimento della firma elettronica - non escludibile a priori, in virtù dei principi generali di difesa e disponibilità delle prove nel processo - non comporterà tuttavia l'onere per la parte che voglia utilizzare il documento di instaurare il procedimento di verificazione, con inapplicabilità degli artt. 214 - 215 c.p.c., e degli effetti sanciti dall'art. 2702 c.c..

La precedente formulazione dell'art.5 DPR 513/97 aveva aperto il varco ad una serie di interpretazioni controverse che oggi parrebbero superate dall'espressa attribuzione del solo requisito legale di **"forma scritta"**.
Occorre precisare a questo punto, per quanto possa sembra ultroneo, che la "forma scritta", nel senso utilizzato dal legislatore non è che un requisito (minimo) di validità della dichiarazione negoziale (quindi in senso sostanziale), al pari di quello previsto per i cd contratti a forma vincolata (es: art.1350 e ss. cod. civ.); assolutamente diverso è il concetto di scrittura privata di cui all'art.2702 cod. civ., quale particolare strumento probatorio documentale, le cui struttura e valenza sono regolate a fini strettamente processuali e non di validità sostanziale.
E' da ritenersi quindi che il riconoscimento del requisito di forma scritta "abiliti" l'applicabilità degli artt. 633 e 634 cpc ai fini della ammissibilità della prova nella fase monitoria, laddove il disconoscimento potrà sempre farsi valere nella fase di opposizione (in questo senso, recentemente: *prof. Giuseppe Olivieri - Relazione illustrata a Napoli, il 14 novembre 2003, nella Giornata di studio Il documento informatico: inquadramento giuridico e funzione notarile, organizzata dalla Assonotai Campania e dall'Istituto Universitario Suor Orsola Benincasa di Napoli)* e, **più in generale, debba inquadrarsi negli effetti ad substantiam del negozio** (o dichiarazione) e cioè conferisca il valore di prova legale (salvi, come detto gli effetti del disconoscimento e della libera valutazione giudiziale) ogni qualvolta la legge preveda il requisito di forma scritta indispensabile per la validità dell'atto (es. trasferimenti immobiliari, prova della simulazione negoziale) e non già al solo fine di escludere l'ammissibilità della prova testimoniale (forma scritta ad probationem tantum, come nel classico caso della prova della transazione, art.1967 cod.civ.).
Si è opposto che tale riconoscimento verrebbe a conferire proprio "alla più leggera delle firme", la forma richiesta per i cd negozi solenni; è da rilevarsi tuttavia che, oltre al tenore testuale della norma, la tesi, pur con le sopradette incertezze, appare proporzionata alla "escalation probatoria" voluta dal legislatore e che non si vedrebbe peraltro quale altro effetto attribuire per primo alla forma minima di firma elettronica, se non quello stesso riconosciuto alla semplice sottoscrizione manuale (non riconosciuta, né autenticata) che pure produce i medesimi effetti sostanziali in ordine ai negozi solenni, con le differenze che sto per evidenziare sul piano probatorio.

Così descritta pertanto la firma elettronica leggera si inquadrerebbe come **un tertium genus** nell'ambito delle prove documentali codicistiche: se infatti, come vedremo, firma digitale ed elettronica avanzata assurgono a rango di scrittura privata riconosciuta, mentre il documento informatico non sottoscritto è equiparabile alle riproduzioni meccaniche e pertanto costituisce piena prova, salvo disconoscimento e conseguente libera valutabilità giudiziale al pari di queste ultime, **non così chiara è la posizione della forma intermedia: il documento sottoscritto con firma elettronica semplice o leggera.**
Da quanto abbiamo premesso apparirebbe infatti una diversa configurazione rispetto alla scrittura privata non riconosciuta: quest'ultima infatti una volta disconosciuta può acquistare valore di prova solo a seguito del vittorioso esperimento della procedura di verificazione, essendo preclusa al giudice ogni diversa valutazione. Al contrario, per la firma elettronica leggera, il legislatore del 2000 non solo ha escluso l'espressa equiparazione alla scrittura privata, ma nel prevedere la libera valutazione giudiziale "tenuto conto delle sue caratteristiche di qualità e sicurezza", **sembrerebbe avere escluso la possibilità di disconoscimento**; fatto inaccettabile per la prevalente dottrina che riterrebbe violati i più elementari principi di difesa garantiti dall'art.24 comma 2 cost..
In questa prospettiva possiamo invece concludere ritenendo che il legislatore abbia voluto assegnare al documento informatico munito di firma elettronica semplice un'efficacia probatoria particolare proprio in considerazione dell'incertezza dell'autenticità della relativa sottoscrizione: **allorquando il documento sottoscritto con firma elettronica semplice non venga disconosciuto, avrà valore di piena prova, mentre qualora venga disconosciuto o comunque contestato, potrà essere liberamente valutabile in giudizio secondo il grado di certezza che la firma può garantire nel singolo caso** (in questo senso: *Francesco Ruscello, Rilevanza dei documenti informatici e tutela dell'affidamento, Vita Notarile n.3 – 2003, 1268 e ss.).*
Secondo altra teoria, non potrebbe parlarsi di vero e proprio mancato disconoscimento, con conseguente valore di scrittura riconosciuta, bensì di mera **mancata contestazione del fatto** (per un'approfondita disamina delle differenze cfr. *Cass., sez. un., 23 gennaio 2002, n. 761, in Foro it., 2002, I, 2019, con nota di C.M. CEA e commento di PROTO PISANI, Allegazione dei fatti e principio di non contestazione nel processo civile, in Foro it., 2003, I, 604 ss. Così anche: Prof. Giuseppe Olivieri, l'Efficacia probatoria del documento informatico - Relazione illustrata a Napoli, il 14 novembre 2003, già cit.)*

c) documento informatico, sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata e/o qualificata

"...*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".*
Venuto meno, con il richiamo all'art.2702, ogni riferimento all'onere di riconoscimento o disconoscimento della sottoscrizione (e del collegato procedimento di verificazione), la pienezza della prova conferita al documento informatico sottoscritto con firma digitale può essere messa in discussione soltanto mediante l'esercizio della **querela di falso.**

L'efficacia di piena prova del documento sottoscritto con firma digitale deve intendersi riferita unicamente alla **provenienza** dell'atto, con la logica conseguenza secondo cui **il contenuto** sarà in ogni caso sottoposto al principio della libera valutazione (art. 116 c.p.c.), sicché ogni mezzo di prova potrà essere utilizzato per dimostrarne il contrario.
Tuttavia è da osservare che – garantendo le specifiche tecniche relative alla *firma digitale* o a quella *elettronica avanzata* anche l'integrità del documento informatico – si è ipotizzato

che la piena efficacia probatoria quanto alla provenienza debba valere anche per l'*estrinseco*. La soluzione positiva è stata affermata da chi ha dedotto che il legislatore *minus dixit quam voluit*, dato che la efficacia di piena prova fino a querela di falso, in realtà non riguarda solo la provenienza delle dichiarazioni, ma anche l'integrità del documento informatico sottoscritto con firma digitale o con firma elettronica avanzata. L'opinione troverebbe conferma nelle affermazioni (dottrinali) secondo cui chi riconosce la propria sottoscrizione implicitamente assume la paternità del testo al momento del riconoscimento (LASERRA, *La scrittura privata*, Napoli, 1959, 121; DENTI, *Querela di falso*, in *Novissimo dig. it.*, XIV, Torino, 1968, 664.)
Non appare però allo stato forzabile una interpretazione estensiva dell'art. 6, 3° comma, d. lgt. 10/2002, laddove ne difetta pure la ragion pratica: perché imporre all'accertamento del contenuto del documento il gravoso procedimento in questione quando il migliore strumento probatorio è evidentemente la CTU, sempre esperibile secondo l'art.116 cpc, che rimane comunque la regola generale?
Vi è poi da aggiungere che se si ritenesse la piena efficacia probatoria operante non solo per la provenienza dell'atto, ma anche quanto all'autenticità e integrità del contenuto, si toglierebbe ogni significato **all'autenticazione della sottoscrizione del documento informatico da parte del notaio** (art. 24 d.p.r. 445/2000). In questa precipua funzione deve leggersi, come vedremo, l'istituto specifico, regolato dall'art.24 DPR 445/2000, nel testo vigente.
Del pari, anche gli altri aspetti essenziali – quanto all'efficacia probatoria – e cioè quelli dell'avvenuta **ricezione e spedizione**, nonché della **data e dell'ora di formazione, di trasmissione o di ricezione** del documento informatico (di cui all'art.14 TU) non risultano coperti dalla piena efficacia probatoria di cui al citato art.10 comma 3 e saranno quindi rimessi al principio della libera valutazione (art. 116 c.p.c.).

Si discute ancora dell'equiparazione sul piano probatorio del documento sottoscritto con firma digitale con le scritture legalmente **riconosciute** (artt. 2702, 2703 c.c., 215 c.p.c.): riteniamo che la risposta debba darsi in senso positivo, all'indispensabile condizione normativa che la firma sia basata su di un **certificato qualificato**, e quindi con esclusione delle altre condizioni previste per le scritture private (riconoscimento, autenticazione, contumacia, mancato disconoscimento).

Esperibilità della querela di falso: la scelta legislativa (nazionale e comunitaria) della "certificazione qualificata" della firma è volta a garantirne autenticità e genuinità al fine della realizzazione del **principio dell'apparenza imputabile**, stante il rischio oggettivo che la firma elettronica possa essere apposta da chi non ne è titolare, dato che essa non potrà mai dirsi direttamene connessa con la persona fisica di quest'ultimo, come la smart card non potrà mai appartenere al titolare quanto la sua mano.
Alla luce di tale principio, non può parlarsi di querela di falso quando si contesti la sussistenza dei requisiti essenziali della firma, come la corrispondenza fra le due chiavi o la mancanza del certificato: queste ipotesi sono equiparabili a quella in cui il nome del firmatario del documento risulti diverso da quello del preteso titolare della firma tradizionale. E' evidente che in questo caso sarebbe sufficiente una ordinaria eccezione di contestazione, esperibile peraltro anche d'ufficio dal Giudice. Secondo alcuni autori si tratterebbe comunque di una forma di disconoscimento, che porterebbe alla "conversione" della firma digitale in firma semplice, suscettibile di disconoscimento senza dar luogo a querela.
La querela di falso è invece esperibile quando:
- un terzo utilizzi abusivamente la chiave privata essendone entrato in possesso con il consenso del titolare;

- un terzo utilizzi abusivamente la chiave privata essendone entrato in possesso fraudolentemente;
- un terzo utilizzi abusivamente la chiave privata per mancata adozione da parte del titolare delle misure di diligente custodia della medesima.
La tutela del firmatario non può essere evidentemente assoluta. Trattasi, con tutta evidenza dell'applicazione nel caso concreto del **principio dell'affidamento per la tutela del terzo incolpevole che abbia fatto affidamento sull'autenticità della firma** (la controparte processuale che ha esibito il documento).
Ora è evidente che nella valutazione del bilanciamento fra gli opposti interessi, l'affidamento incolpevole potrebbe essere privilegiato nel primo e nel terzo caso, mentre solo nel secondo deve ritenersi prevalente e meritevole di tutela l'interesse del titolare della firma cui la chiave sia stata sottratta fraudolentemente.
In questo caso il titolare della firma potrà dimostrare la falsità e l'inefficacia e/o invalidità dell'atto in questione, **per non aver egli manifestato alcuna volontà**, con conseguente declaratoria di inefficacia e/o invalidità del negozio.
Quale sarà in questo caso la tutela incolpevole del terzo?
- qualora si renda nota l'identità del **falsificatore** e il suo comportamento colposo sarà quest'ultimo a risarcire i danni al terzo;
- diversamente, qualora l'uso abusivo dovesse dipendere da colpa del **certificatore** sarà quest'ultimo a rispondere dei danni;
- nel caso invece in cui non sia individuabile una responsabilità di un falsificatore o del certificatore la dottrina si è posta il problema dell'individuabilità di una **responsabilità oggettiva** gravante sul titolare della firma per garantire la tutela dell'affidamento del terzo incolpevole. La teoria non è dimostrabile. E' più corretto ritenere che l'eventuale obbligo risarcitorio nei confronti del terzo possa rilevare sotto il profilo **dell'inadempimento dell'obbligo di diligente custodia e di adozione delle misure di sicurezza organizzative e tecniche** (artt. 28 e 29-bis DPR 445/2000, recentemente integrate da quelle previste nel DPR 13.1.2004), venendo il medesimo chiamato a dare la prova liberatoria di non aver potuto impedire il fatto (art.2048 e 2054 cc e/o di avere adottato tutte le misure idonee ad evitare il danno (2050) o il caso fortutito (2051 o 2052), che rappresentano peraltro le ipotesi normative di prova liberatoria anche nelle specifiche fattispecie tipiche di responsabilità oggettiva, ove prevista.
Secondo un'altra teoria (ma si tratta solo di ipotesi *de iure condendo*) il "rischio" dovrebbe invece accollarsi a chi ha fatto affidamento sulla validità ed efficacia della firma, in base ad un non meglio specificato **"dovere di prudenza"** oppure venire a ripartirsi fra i diversi soggetti coinvolti.

Il Procedimento è regolato dagli artt. 221 ss., con particolare considerazione alla necessità dell'*interpello* della parte che ha prodotto il documento informatico; all'obbligatorio intervento del P.M.; alla competenza inderogabile del tribunale; alla necessità del giudizio in composizione collegiale (art. 50 *bis* c.p.c., 1° comma, n. 1).

La specificità del *documento informatico* comporta evidentemente anche la peculiarità delle **indagini di fatto** richieste per stabilire la fondatezza o meno della querela.
Nel caso di sottoscrizione con ***firma digitale*** – offrendo il sistema una presunzione assoluta di conformità alla legge – chi propone la domanda, per evitare di vedersi riconosciuto autore del documento, dovrà provare le singole circostanze normative previste dall'art.23, ed esemplificativamente: - che altri soggetti erano a conoscenza e/o potevano avere accesso alla sua firma digitale; - che la chiave pubblica corrispondente alla chiave privata adoperata era stata oggetto dell'emissione di un certificato qualificato scaduto di validità ovvero revocato o sospeso; - che, in caso di revoca o sospensione

dell'efficacia del certificato elettronico, l'abuso della firma era avvenuto dopo la pubblicazione della revoca o sospensione o comunque che l'altra parte ne era a conoscenza.

Come si vede, il giudizio di fatto richiesto per la querela di falso del documento informatico – a differenza della querela tradizionale – **offre largo spazio alla prova libera** e perfino, qualora si tratti di stabilire se chi (in aggiunta al titolare) era a conoscenza della firma digitale ne abbia fatto uso o meno, ad **argomenti di prova o a presunzioni (semplici)**.
Nel caso di sottoscrizione con la ***firma elettronica avanzata***, la querela potrà fondarsi, oltre che sulle circostanze appena indicate, anche sulla non conformità del sistema tecnologico adottato ai protocolli normativi.
In questi casi, la raggiunta prova della mancanza della *piena* efficacia probatoria, non potrà comunque escludere la "*rilevanza giuridica né ammissibilità come mezzo di prova*" (cd principio di conservazione: art. 6, 4° comma, d. lgt. 10/2002) del documento, che dovrà essere oggetto di libera valutazione quanto al contenuto e alla provenienza.

Poiché – per le ragioni prima illustrate – è parso corretto ritenere che l'efficacia di *piena prova* della *firma digitale* (o *elettronica avanzata*) abbia a oggetto (unicamente) la provenienza dell'atto, consegue che **il contenuto sarà in ogni caso sottoposto al principio della libera valutazione (art. 116 c.p.c.), sicché ogni mezzo di prova potrà essere utilizzato per dimostrarne il contrario.**
Infine – poiché la certificazione della *firma digitale* (o *elettronica avanzata*) è sottoposta al termine iniziale e finale del periodo di validità in essa indicato ai sensi dell'art. 27 *bis*, 1° comma, lett. *f*, d.p.r. 445/2000 – **l'efficacia probatoria del documento potrà operare soltanto nell'arco temporale compreso fra i due termini**.

****

Solo un cenno, per concludere, possiamo dedicare al **documento informatico con firma digitale autenticata.**
L'art. 24 fa riferimento esplicito alla *firma digitale*, ma può sostenersi l'applicabilità dell'autenticazione notarile anche al documento informatico sottoscritto con altro tipo di *firma elettronica avanzata*, vista la completa equiparazione tra le due firme, operata dall'art. 6, 3° comma, del d. lgt. 10/2002, mentre l'effetto probatorio sancito dall'art. 24 del d.p.r. 445/2000 non può dirsi applicabile al documento sottoscritto con la firma elettronica semplice.

Secondo una recente interpretazione, ancorché nessuna norma contempli **l'atto pubblico informatico**, il documento in esame assumerebbe la medesima efficacia probatoria sancita (per l'atto cartaceo) dall'art. 2700 c.c. L'unica differenza fra i due tipi di documenti sarebbe costituita dai **limiti temporali di validità** (soprattutto per ciò che concerne il termine finale) operanti per l'atto informatico. L'argomento ha trovato soddisfazione nella *Relazione illustrata a Napoli, il 14 novembre 2003, Giornata di studio Il documento informatico: inquadramento giuridico e funzione notarile, organizzata dalla Assonotai Campania e dall'Istituto Universitario Suor Orsola Benincasa di Napoli, dal Prof. Giuseppe Olivieri. l'Efficacia probatoria del documento informatico.*
Si è opposto tuttavia, oltre la mancanza di richiamo testuale, anche che la contestuale formazione dell'atto alla presenza delle parti e del Notaio, postulata dall'art.2700 c.c., non è compatibile con la fattispecie in oggetto.

La funzione probatoria che l'art. 24 del d.p.r. 445/2000 (in combinato disposto con le norme concernenti la *qualificazione* e la *validazione* temporale della firma digitale o elettronica avanzata) affida al documento in esame si risolve nella prova – controvertibile soltanto con la querela di falso avverso le relative attestazioni notarili – della: a) provenienza della firma digitale da suo titolare, preventivamente identificato; b) validità della chiave (o della certificazione) utilizzata; c) dichiarata corrispondenza tra la volontà espressa nel documento e quella che s'intendeva manifestare; d) non contrarietà dell'atto all'ordinamento giuridico a norma della legge notarile (assenza di vizi cagionanti la nullità); *e*) provenienza dell'atto dal pubblico ufficiale; *f*) data.

L'intervento del notaio assumerebbe perciò la funzione di restringere o comunque modificare l'oggetto del possibile giudizio di falso instaurato contro il documento informatico. Infatti, ove venga prodotto in giudizio un documento informatico con firma digitale autenticata, **la parte contro cui è prodotto potrà proporre querela di falso per far valere la mendacità delle dichiarazioni del pubblico ufficiale**, non per far valere semplicemente che la sua chiave privata è stata abusivamente o fraudolentemente utilizzata da altri a sua insaputa. Ciò comporta, indubbiamente, un rafforzamento della tenuta probatoria del documento informatico sottoscritto con firma digitale autenticata.
E' infine da ribadire che il 2° comma dell'art. 24 del d.p.r. 445/2000 precisa che il notaio (o il pubblico ufficiale rogante) debba attestare anche – evidentemente raccogliendo una dichiarazione in tal senso – **che la volontà manifestata nel documento informatico sottoscritto sia esattamente quella che si intendeva manifestare**.
E' quindi evidente che la fede privilegiata assisterà non la reale corrispondenza fra la volontà manifestata e quella interna (che come già detto sarebbe questione probatoria attinente alla simulazione negoziale), ma il fatto che la parte ha esplicitamente affermato l'indicata corrispondenza.

****

Alla luce delle poche note esposte, il documento informatico, nelle diverse tipologie normative, acquista quindi una rilevanza processuale graduata e poliedrica, in cui possiamo sostanzialmente riconoscere da una parte un rafforzamento generale del potere di libera valutazione giudiziale, cui corrisponde dall'altra l'ampliamento delle circostanze fattuali e dei relativi accertamenti tecnici oggetto della prova, rispetto alle fattispecie probatorie documentali codicistiche.

*** Marisa Bonanno** - Avvocato del Foro di Verona.
Curatore e responsabile del sito di informazione giuridica http://www.studiumfori.it/. Moderatore della mailing list Deontologia Forense http://it.groups.yahoo.com/group/DeontologiaForense/ . Componente del Consiglio Direttivo del Circolo dei Giuristi Telematici http://www.giuristi.thebrain.net/circolo/ .

E-MAIL E PROVA NEL PROCEDIMENTO MONITORIO

di Luca Giacopuzzi – Avvocato in Verona

www.lucagiacopuzzi.it

Solo una quindicina di anni fa il personal computer era uno strumento a metà tra il tecnologico e l'esoterico. Uno strumento per molti "ostico", al più impiegato unicamente come un surrogato della macchina da scrivere. Poco (e male) utilizzato, quasi temuto.

Poi l'avvento su larga scala di Internet ha segnato una svolta, imprimendo una forte accelerazione allo sviluppo delle tecnologie e all'impiego di esse nella vita quotidiana.

Oggi, per esempio, tutti utilizzano (o, per lo meno, conoscono) Internet e la posta elettronica.

Proprio l'e-mail (meglio: il valore probatorio dell'e-mail) è stata recentemente al centro di un vivace dibattito dottrinale, una "querelle" – dai toni a volte accesi – ben lungi dall'aver trovato una risposta definitiva ed appagante.

Questi, in estrema sintesi, i termini della questione. La posta elettronica – è stato sostenuto – costituisce un documento informatico sottoscritto con firma elettronica "semplice", dato che "il mittente, per poter creare ed inviare detta e-mail, deve eseguire un'operazione di validazione, inserendo il proprio username e la propria password".

Lo ha stabilito il Tribunale di Cuneo, con un provvedimento innovativo, nel quale – facendo leva sull'art. 10, comma 2, del TUDA, DPR 445/00 ("Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta") – è stato concesso un decreto ingiuntivo a fronte di un credito la cui prova è stata data unicamente a mezzo e-mail (Tribunale Cuneo, decreto 15.12.2003 n. 848).

Ripercorriamo quindi, seppur rapidamente, la ricostruzione giuridica che parte ricorrente ha abilmente offerto al Giudice a sostegno delle proprie ragioni.

- L'e-mail rappresenta un "documento informatico", che – ai sensi dell'art.8 TUDA – è valido e rilevante a tutti gli effetti di legge;
- Il documento informatico, se sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta;
- La posta elettronica è documento sottoscritto da firma elettronica , perché il mittente, per poter creare e spedire il messaggio, deve eseguire un'operazione di validazione, consistente nell'inserimento del proprio username e della propria password;
- In un ricorso per decreto ingiuntivo, pertanto, la prova del credito può essere utilmente data anche mediante la produzione di e-mail.

Il provvedimento del Tribunale di Cuneo, che – come detto – ha concesso il decreto è stato salutato con favore da parte di certa dottrina, che ha fatto proprie le tesi esposte nel ricorso.

Tra i primi – e più brillanti – commentatori del decreto va segnalato l'Avv. Lisi (autore di molti contributi, ben argomentati, sul punto; vedasi ad esempio: "L'e-mail dal commercio elettronico alle aule di giustizia" su www.scint.it/appr_new.php?id=87 o "Essere o non essere: i moderni dubbi amletici di una e-mail anonima" su www.scint.it/appr_new.php?id=98).

Sulla scia dell'avvocato leccese, poi, altri studiosi (es. Amendolagine) hanno avuto parole di apprezzamento per il per l'operato del giudice piemontese, recependo nei propri scritti la tesi del ricorrente.

Tesi indubbiamente lucida, sorretta da argomentazioni ben concatenate le une alle altre, che sembrerebbe ineccepibile. Ho usato, però, il condizionale ("sembrerebbe"), e non a caso. Ritengo, infatti, che un approccio diverso alla normativa di riferimento possa schiuderci scenari differenti.

Le mie perplessità, beninteso, non sono nei confronti della strategia difensiva adottata dal Collega (che, anzi, bene ha fatto ad incunearsi nelle pieghe di norme infelici, per ottenere un risultato a sé favorevole!), ma sono rivolte nei confronti di un decreto forse concesso con troppa "superficialità". Da parte, cioè, da un giudice che ha sposato troppo frettolosamente la tesi del ricorrente, pur se esposta in modo accattivante.

Il problema non è nuovo, specie nel diritto di Internet, settore nel quale la corretta analisi giuridica si associa necessariamente ad una corretta comprensione del fenomeno da un punto di vista tecnico e fattuale (chi si ricorda – tanto per fare un esempio - quanto avvenne qualche anno fa in tema di nomi a dominio, con le bizzarre pronunce della "scuola toscana"?).

Ma non divaghiamo, e torniamo quindi al tema oggetto della presente relazione, per dar conto delle perplessità che – come accennavo – la lettura del decreto ha in me suscitato.

Una considerazione, preliminare ad ogni altra osservazione.
La questione sul valore probatorio dell'e-mail in un procedimento monitorio si pone qualora la mail sia l'unica base documentale sulla quale è stato concesso il D.I.

Nulla quaestio, invece, quando la mail sia utilizzata "a supporto" di altra produzione documentale (fatture, ddt, corrispondenza), dato che anche all'e-mail – in quanto documento informatico – può ben essere dato ingresso in giudizio, ai sensi e per gli effetti di cui all'art. 2712 c.c.

Il problema circa il valore probatorio di un e-mail è, insomma, racchiuso nel seguente quesito, al quale bisogna dare una risposta: la mail è un documento informatico sprovvisto di qualsivoglia firma elettronica e perciò equivalente ad una mera riproduzione meccanica (art. 2712 c.c.) ovvero è un documento informatico provvisto di firma elettronica "debole"?

Questo, in buona sostanza, il nocciolo della questione, perché se si riesce a dimostrare che l'e-mail è sottoscritta con firma elettronica, si potrà agevolmente sostenere che essa riveste forma scritta. L'art. 10, comma 2, TUDA, infatti, afferma a chiare lettere che "il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta".

Ci si deve allora chiedere "se" vi sia (e, in caso affermativo, "dove" sia) la firma elettronica in una mail.

Secondo la tesi del ricorrente, la firma elettronica sarebbe costituita dall'inserimento di "username" e "password" immessi per accedere al server SMTP, server che bisogna utilizzare per inviare un messaggio di posta.

La tesi, pur se suggestiva, non è a mio avviso esatta. Per comprenderne appieno le ragioni, leggiamo cosa si intenda per firma elettronica nel testo vigente. L'art. 1, comma 1, lett.cc) DPR 445/00 definisce la firma elettronica come:

- l'insieme dei dati in forma elettronica

- allegati oppure connessi tramite associazione logica ad altri dati elettronici
- utilizzati come metodo di autenticazione informatica

Nessun dubbio che username e password costituiscano un insieme di dati in forma elettronica, ma la firma elettronica richiede anche che essi siano "allegati oppure connessi tramite associazione logica ad altri dati elettronici", che sono appunto quelli che devono essere validati.

Nulla di tutto questo avviene nella fase di invio di una mail. Detto altrimenti – ed in termini più semplici – non si può parlare di firma elettronica perché manca la connessione logica tra i dati validanti (combinazione di username e password) e i dati da validare (i dati, cioè, che costituiscono il messaggio e-mail).

Ciò è stato ben compreso da attenta dottrina (per tutti: Cammarata, in "Un messaggio e-mail non è prova scritta" in www.interlex.it/docdigit/provascritta.htm), che aggiunge: "La connessione logica avviene attraverso la procedura – logica – che calcola l'impronta dei dati da validare e la cifra con la chiave privata del firmatario".

Mi si permetta, su quest'ultima osservazione, di nutrire qualche dubbio sull'esattezza di quanto (pur autorevolmente) sostenuto. Ritengo, infatti, che la "connessione logica" deve essere vista come la possibilità di ricondurre in modo univoco i dati del documento ai dati del firmatario, senza però dover (o poter) impiegare alcuna forma di "elaborazione o calcolo di hash", anche perché in questo caso si ricadrebbe nell'ipotesi di firma elettronica "avanzata" (così, tra l'altro, Caccavella).

Quindi se il documento è firmato con un sistema informatico che permette di ricondurre il documento stesso all'autore e se detto autore è identificato tramite l'inserimento di credenziali di autenticazione (es. username e password) ritengo che si possa parlare di firma elettronica.

Ma ciò – ed è questo il punto – non avviene nella fase di invio di un'e-mail, perché per inviare un messaggio di posta elettronica non occorre essere autenticati dal server SMTP e, più importante ancora, l'immissione di username e password non comporta alcuna connessione logica tra questi dati (d. validanti) e quelli che costituiscono il messaggio e-mail (d. da validare). Ragionando diversamente – per dirla con Cammarata – "sarebbe come affermare che quando si deve inserire una password per accedere a un PC, tutti i documenti contenuti in quella macchina hanno la firma elettronica".

La ricostruzione giuridica posta a base del decreto ingiuntivo del Tribunale di Cuneo, allora, non regge.

Non è in altre parole accettabile l'assunto secondo il quale è firma elettronica qualsiasi tecnica utilizzabile come metodo di autenticazione informatica.

Accedendo a questa impostazione – come osservato anche da Navone – anche un SMS sarebbe un documento informatico munito di firma elettronica debole. Il mittente che voglia inviare un SMS, infatti, per accedere alla rete telefonica deve "autenticarsi" (digitando il proprio PIN sulla carta SIM).
Seguendo questa tesi, dunque, soddisferebbe il requisito legale della forma scritta ad substantiam una compravendita immobiliare conclusa via SMS, tramite un mezzo – cioè – che certo non favorisce quella "ponderazione del consenso" che la legge vuole assicurare laddove prevede oneri formali (si consideri, tra l'altro, che il linguaggio adoperato negli SMS è di norma più simile a quello parlato che a quello scritto, o comunque molto "friendly", come testimonia il largo impiego degli emoticons).

L'esempio dà a mio avviso la misura dell'erroneità della tesi posta a base del provvedimento concesso a Cuneo.

Non posso, allora, che manifestare le mie perplessità sulla tesi (abilmente) prospettata per ottenere l'invocato decreto ingiuntivo.

Nel ricorso si legge testualmente: "E'pacifico che l'e-mail costituisca un documento informatico sottoscritto con firma elettronica, in quanto il mittente, per poter creare ed inviare detta e-mail, deve eseguire un'operazione di validazione, inserendo il proprio username e la propria password".

Altri commentatori (Amendolagine) si esprimono in termini sostanzialmente analoghi: "per poter accedere ad un determinato indirizzo e-mail…bisogna prima conoscere (al fine di poterli utilizzare) i dati identificativi appartenenti ai soggetti interessati alla connessione".

L'assunto è suggestivo, ma è smentito dal dato tecnico.

A parte l'improprietà terminologica (nel ricorso, infatti, si parla di operazione di "validazione" con riferimento ad un processo di "autenticazione"; i due termini, in realtà, si riferiscono a concetti ben distinti), va osservato che per inviare un'e-mail non occorre essere autenticati dal server SMTP; non occorre, cioè, conoscere e quindi utilizzare lo username e la password associati all'indirizzo di posta elettronica che viene utilizzata come mittente.

Un semplice esempio – che spero possa chiarire ciò che vado dicendo – avvalendomi di una mail che ho ricevuto.

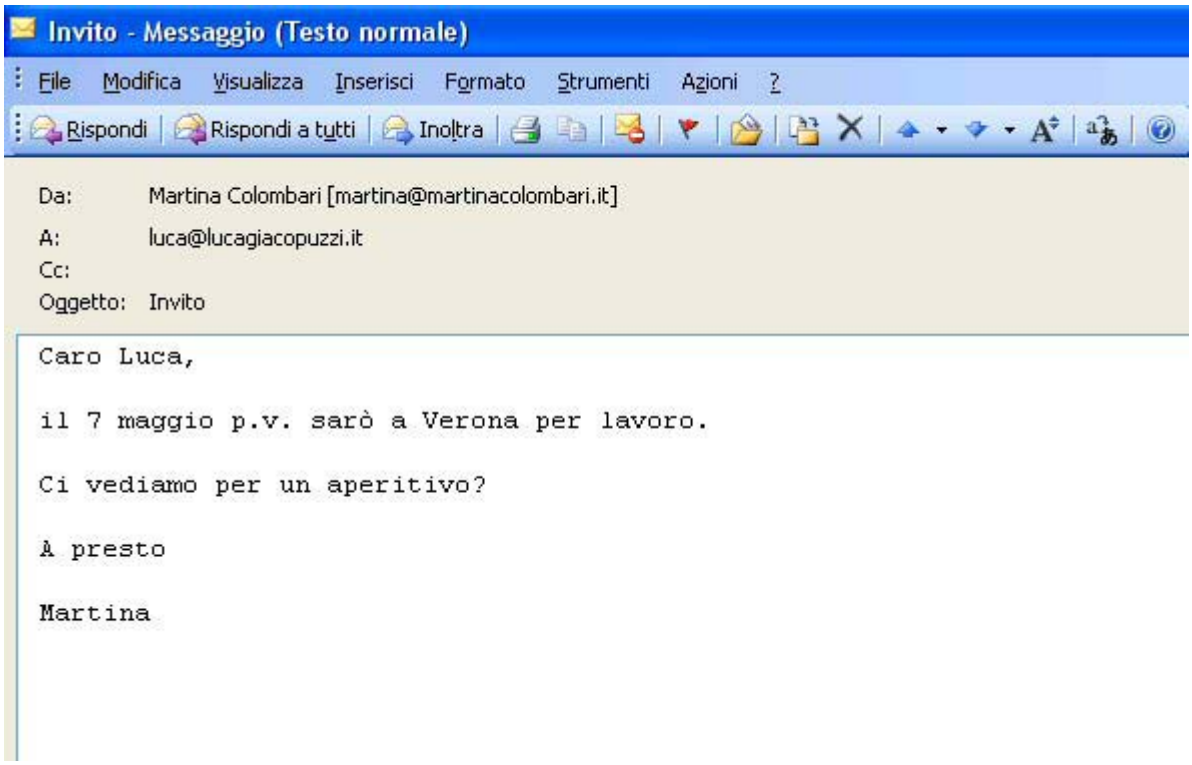

Fig.1 (Fake mail)

Come si vede chiaramente dalla figura, la mail è stata indirizzata a luca@lucagiacopuzzi.it da martina@martinacolombari.it. Non c'è alcun dubbio: così si legge nei relativi "campi".

Ma è stata davvero la Colombari ad inviare la mail? No, no di certo; è stato in realtà facile inviare la mail pur non conoscendo username e password che Martina Colombari usa per accedere alla sua casella di posta. Ciò a dire, in altre parole, che l'invio del messaggio di posta è stato possibile in assenza di autenticazione.

Se così è, la tesi secondo la quale la mail costituirebbe "documento informatico sottoscritto con firma elettronica, in quanto il mittente, per poter creare ed inviare detta mail, deve eseguire un'operazione di validazione" non regge al cospetto del dato tecnico, oltre che – come osservato in precedenza – anche di quello giuridico (in quanto non c'è quella "connessione logica" tra dati validanti e dati da validare che la legge pretende perché si possa parlare di "firma elettronica").

Sia ben chiaro: non sto demonizzando l'impiego dell'e-mail (lungi da me), né sono pregiudizialmente ostile all'ingresso di essa nelle aule di giustizia.

Semplicemente, ritengo che l'e-mail non soddisfi il requisito legale della forma scritta, dato che nel procedimento di invio di un messaggio per posta elettronica a mio avviso non c'è traccia di "firma elettronica". I server SMTP, infatti, non eseguono alcuna autenticazione del mittente e manca del tutto la connessione logica tra dati validanti (combinazione di username e password) e dati da validare (i dati, cioè, che costituiscono il messaggio e-mail) che la normativa vigente (TUDA) richiede alla firma elettronica.

L'e-mail, in conclusione, ai sensi dell'art. 10, comma 1, TUDA, avrà – in quanto documento informatico – l'efficacia probatoria prevista dall'art. 2712 c.c. riguardo ai fatti ed alle cose rappresentate. Un'efficacia probatoria molto debole, in quanto subordinata al comportamento processuale del soggetto contro il quale il documento è prodotto. Tale soggetto, in ogni caso, avrà comunque l'onere di disconoscere il documento se vuole impedire che lo stesso produca l'effetto di una piena prova.

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO
Problematiche
di formazione e probatorie

EMAIL, FIRMA ELETTRONICA E FORMA SCRITTA

INTERVENTO NEL CONVEGNO
"DOCUMENTO INFORMATICO: PROBLEMATICHE DI FORMAZIONE E PROBATORIE"

VERONA, 7 MAGGIO 2004

AVV. MARCO CUNIBERTI

Ha suscitato recentemente molto scalpore la notizia di un decreto ingiuntivo, che il Tribunale di Cuneo ha concesso - ex art. 634 c.p.c. - sulla base di una ricognizione di debito contenuta in una normale email, accogliendo la tesi secondo cui, alla luce della normativa in tema di documento informatico, anche la email "semplice" si può considerare sottoscritta con firma elettronica, così soddisfando il requisito legale di forma scritta.

L'art. 10, comma 2, del DPR n. 445/00 prevede infatti che "*Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta*", benchè "*sul piano probatorio il documento stesso è liberamente valutabile*": pertanto, il documento informatico sottoscritto con tale "firma" è sufficiente quando la legge richieda espressamente la forma scritta per la validità dell'atto (cd. *ad substantiam*) o per la validità di una prova ivi contenuta (cd. *ad probationem*), salve contestazioni sull'autenticità del documento (ma questo riguarda il piano probatorio, per il quale, correttamente, la legge da al Giudice la più ampia libertà di valutazione).

Di conseguenza, se la normale email contenente la ricognizione di debito si può considerare un documento informatico sottoscritto con firma elettronica, benchè "leggera", ben potrà allora essere concesso il Decreto Ingiuntivo.

Occorre quindi per prima cosa chiedersi se la email sia un documento informatico, che l'art. 1, comma 1, lett. b) del DPR definisce "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*": ed essendo la email proprio la rappresentazione informatica di tante cose, tra cui una dichiarazione di volontà o di scienza, essa riveste certamente le caratteristiche richieste dalla norma.

Per quanto riguarda, poi, la firma elettronica, l'art. 1, comma 1, lett. cc), stabilisce che questa sia "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica*".

Ora, poichè appare ovvio che la definizione "sottoscrizione" costituisca, per quel che riguarda un documento informatico - e quindi la rappresentazione grafica di dati - una fictio juris (in quanto in nessun caso si sottoscrive materialmente alcunchè, neppure con la firma digitale, che corrisponde

invece all'inserimento, da parte di qualcuno - quasi sempre diverso dall'effettivo titolare - di una smart card e della digitazione di un PIN, che non viene certo riportato nella mail), sembra logico che l'espressione "documento informatico sottoscritto con firma elettronica" possa anche esser interpretata con "firma elettronica apposta (o allegata) al documento informatico".

E' quindi necessario che al documento informatico sia più che altro allegata una firma elettronica, dev'esservi contenenuta, in modo che il destinatario se ne possa accorgere.

L'email deve pertanto contenere un insieme di dati in forma elettronica, i quali siano allegati oppure connessi - tramite associazione logica - ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Prima di analizzare la sussistenza o meno di tali requisiti, è opportuno ulteriormente puntualizzare che la norma non chiede assolutamente che questa "firma" sia sicura, certa, infalsificabile: esattamente come la dichiarazione contenuta in un foglietto di carta firmato (che costituisce comunque forma scritta, indipendentemente dal fatto che la firma sia falsa o comprensibile), si richiede solo che questa firma ci sia ed abbia i requisiti di legge.

L'email contiene (oltre eventualmente la firma, "l'indicazione grafica" del mittente, in fondo alla mail stessa, che ai nostri fini non serve ad alcunchè, anche se potrebbe avere rilevanza ai fini penali, ex art. 491 bis c.p.) un indirizzo di provenienza (es. mariorossi@libero.it, che ci dice - a parte il fatto che possa essere falsificata - che essa è o dovrebbe esser stata inviata da un indirizzo creato presso un provider di posta elettronica) e sopratutto gli headers: sono questi una serie di dati precisi, contenenti numerose informazioni (molte più di quante possano esser contenute in uno sconosciuto foglio di carta!), tra cui tutto il percorso della email, l'indirizzo IP di provenienza (cioè a quale utenza telefonica era collegato il computer mittente) e, soprattutto, da quale ISP (Internet Service Provider) provenga.
In pratica, l'insieme di dati dati indirizzo-headers indica chiaramente che l'email proviene (o dovrebbe comunque provenire) da un'area riservata di un ISP (che cioè, per essere inviata, occorreva aver accesso a quell'area riservata), nonché il momento di invio e l'IP, da cui si può risalire addirittura alla macchina che me l'ha mandata.

Passando al secondo requisito, non si può negare che un sistema di autenticazione costituito da un codice per l'identificazione dell'incaricato (username) ed una parola chiave riservata a questo associata (password) costituisca un metodo di autenticazione informatica; l'espressa conferma viene oltretutto dal nuovo Tasto Unico in materia di tutela dei dati personali (DLgs 196/2003), che ha espressamente specificato quanto sopra agli artt. 1 e 2 dell'allegato B.

Come si è visto, l'insieme di dati dati indirizzo-headers dice che quella data email è stata scritta da qualcuno che ha dovuto (o avrebbe dovuto) necessariamente, per scriverla, inserire un ID e una PW; o, meglio, che chi l'ha scritta, non può non aver inserito un ID ed una PW.
Perciò, grazie al suddetto insieme di dati, si sa che per scrivere quella email è (o avrebbe docuto essere) stato utilizzato un sistema di autenticazione informatica.

A questo punto, non si può negare che ci sia una connessione logica, un'associazione di idee tra l'insieme di dati indirizzo-headers (contenuti nella email ricevuta) ed il metodo di validazione necessariamente (condicio sine qua non) utilizzato.
Logica conseguenza, a questo punto, è che anche la email "semplice", contenendo tutte le caratteristiche di legge, costituisca un vero e proprio documento informatico munito di firma elettronica (benchè "leggera") e, pertanto, la dichiarazione di volontà o di scienza ivi contenuta rivesta la forma scritta.

In relazione al ragionamento sin qui esposto sono state sollevate alcune interessanti eccezioni, cui sono però state date - quantomeno a parere di chi scrive - soddisfacenti risposte.

In primis, è stato sostenuto che, poiché usando un client di posta (cioè un programma come MS Outlook Express) per inviare una email non viene effettuata alcuna autenticazione (in pratica, per raggiungere il server "dedicato all'invio" del proprio provider, cd. SMTP, al programma non viene richiesta l'immissione di username e password, cosa che invece lo stesso programma effettua automaticamente quando verifica la posta in arrivo), non sussisterebbe la connessione logica con il sistema di autenticazione informatica.
E' però agevole ribattere che, in primis, così ragionando si ammette implicitamente che la cd. "webmail" (cioè l'invio di posta elettronica accedendo direttamente, via web, al provider che fornisce la casella di posta, non utilizzando alcun programma specifico) ha invece tutti i requisiti, benchè si tratti comunque di una email normalissima.
L'eccezione non reggerebbe inoltre per le email cd. "di risposta" (cioè quelle che rispondono ad un'altra email ricevuta, le quali contengono anche il contenuto della stessa email cui si intende rispondere), ove si è addirittura sicuri che l'autore della risposta è proprio colui che ha ricevuto la prima email, il quale ha dovuto certamente autenticarsi per leggerla (per poi rispondere).
Ma, soprattutto, l'eccezione è infondata anche per il caso di utilizzo del programma di posta: anche se, infatti, non ci si autentica in quella specifica occasione, si utilizza però un identificativo (l'indirizzo del mittente) che si riferisce comunque a un'area riservata, creata apposta e quindi protetta dal suddetto metodo di autenticazione (in pratica, se ci arriva una email dall'indirizzo mariorossi@libero.it, siamo convinti che chi l'ha inviata abbia l'uso esclusivo della relativa area riservata, protetta da un sistema di autenticazione informatica costituito da username e password; in caso contrario - se cioè il mittente inserisse appositamente nel suo client un indirizzo che non esiste, come ad esempio francorossi@libero.it, approfittando del fatto che non è richiesta l'autenticazione e facendo così credere falsamente al destinatario che arriva da quell'inesistente account - commetterebbe un illecito ex art. 491 bis c.p., poichè chiunque crederebbe che quell'account esiste, cioè esista un'area riservata al relativo titolare): pertanto, la connessione logica, l'associazione di idee tra l'insieme indirizzo-headers di quella email e l'utilizzo di dati di autenticazione non viene a mancare, anche se in quel caso concreto non erano stati immessi.
La firma, è infatti costituita dall'insieme indirizzo-headers (che ben sussiste anche nella email inviata dal client), non dall'insieme di dati username-password, cui i primi possono anche soltanto essere "connessi tramite associazione logica".
Qualsiasi problema si risolverebbe, in ogni caso, adottando un client di posta che effettui l'autenticazione anche per la posta in uscita.

Altro rilievo è stato mosso in quanto, poiché nel caso di webmail l'autenticazione informatica (cioè l'inserimento di username e password) è effettuata prima di scrivere la email e non dopo, non vi sarebbe una vera e propria firma del documento informatico.
Ciò non corrisponde però al vero, poichè - come si è visto - la firma è costituita dall'insieme di dati indirizzo-headers (e non dall'insieme username-password), che viene apposto alla email al momento dell'invio e che deve soltanto essere connesso logicamente al sistema di autenticazione informatica.
In ogni caso, l'eccezione appare di poca consistenza, considerato che, pur parlandosi di "firma" e di "sottoscrizione", è chiaro che si utilizzi una fictio iuris e ci si riferisca materialmente a qualcosa di diverso.

Per quanto invece riguarda le eccezioni sulla obbiettiva insicurezza della email, la quale sarebbe agevolmente falsificabile, si risponde che il legislatore ha correttamente parlato soltanto di "requisito legale" di forma scritta (così come è in forma scritta anche una promessa di pagamento

scritta sul retro di un biglietto del tram, con in calce una firma qualsiasi), mentre per quanto riguarda l'efficacia probatoria ha lasciato libera valutabilità al Giudice che eventualmente dovesse occuparsi del caso concreto.
D'altronde, gli stessi - se non maggiori - rischi di insicurezza valgono nel caso in cui ci arrivi una lettera cartacea con una carta intestata ed una firma che noi non conosciamo: ebbene, di sicuro è la email, che - ad un'analisi approfondita - può fornirci le maggiori garanzie (si pensi solo a quante informazioni ci sono negli headers, mentre in una lettera si può al limite sapere con certezza da che città è partita).

Le considerazioni sin qui svolte possono rappresentare una svolta nell'attribuzione alla email di un più consono ed adeguato valore legale, anche alla luce del ruolo che ormai tale mezzo di comunicazione riveste: l'invio di email "normali" è infatti oggi il metodo di comunicazione più utilizzato non solo nel commercio elettronico, ma anche nei rapporti commerciali "tradizionali" (tutta la fase precontrattuale e di esecuzione dei contratti - specialmente servizi, appalti, contratti che richiedano continui contatti tra le parti -, gli ordini dei rivenditori ai grossi distributori, ecc., viene fatta via email, lasciando al cartaceo solo la stipula del contratto vero e proprio), per non parlare poi delle specifiche tecniche ed alle comunicazioni interne alle aziende.
Pertanto, in attesa di un'eventuale modifica legislativa, pare corretto sostenere che anche la semplice email soddisfa il requisito legale della forma scritta, pur con tutti i doverosi limiti per quel che riguarda l'efficacia probatoria.

GRUPPO DI INIZIATIVA FORENSE

Verona 7 maggio 2004

DOCUMENTO INFORMATICO

Problematiche
di formazione e probatorie

Il documento informatico "scritto", "firmato", ma non "sottoscritto" nel commercio elettronico internazionale: dall'e-mail all'accesso in un'area riservata del sito web.

(Il presente saggio, arricchito di note e paragrafi, entrerà a far parte del Volume "*Diritto e società dell'informazione - Riflessioni su informatica giuridica e diritto dell'informatica*", AA VV, Myberg Editore, Milano, 2004, in corso di pubblicazione ad opera del CIRCOLO DEI GIURISTI TELEMATICI)

di Andrea Lisi (*)

*****

Fa bene a volte rileggere alcuni passi della letteratura e provare a reinterpretarli alla luce delle innovazioni tecnologiche che travolgono tutte le nostre certezze sociali, economiche, giuridiche. E così alcune suggestive parole di BALDASSARRE CASTIGLIONE ([1]) sul significato dello "scritto" assumono sfumature nuove, innovative e impensate per il periodo in cui sono state elaborate dall'autore: "*lo scrivere non è altro che una forma di parlare, che resta ancor poi che l'uomo ha parlato; e quasi un'immagine, o più presto vita delle parole; e però nel parlare, il qual, subito uscita che è la voce, si disperde, son forse tollerabili alcune cose che non sono nello scrivere*"…voler ancora ritenere che la manifestazione di volontà contenuta in un messaggio di posta elettronica possa non essere ricondotta giuridicamente alla "forma scritta" fa sorridere un po' se si riflette sulla forza evocativa e poetica di certe parole…
In verità, il recente animato dibattito sul valore formale dell'e-mail quale documento "scritto" ai sensi del novellato art. 10 DPR 445/2000 ([2]), andrebbe più correttamente analizzato alla luce

---

(*) Avvocato in Lecce, Studio Legale Lisi (www.studiolegalelisi.it). Titolare, con il dr. Davide Diurisi, dello Studio associato D.&L. (www.studiodl.it), consulenza ICT&International Trade. Curatore del portale www.scint.it. Autore di numerose pubblicazioni in materia di diritto del commercio internazionale e diritto delle nuove tecnologie. Direttore Scientifico del Corso di Alta Formazione in Diritto & Economia del Commercio Elettronico Internazionale (www.scint.it/altaformazione) e docente in Master universitari dedicati al diritto delle nuove tecnologie.

([1]) Baldassarre Castiglione (Casatico 1478, Toledo 1529), intellettuale della media nobiltà dell'epoca e autore de *Il Cortegiano*.

([2]) Il dibattito ha preso il via dalla pubblicazione sul web del decreto ingiuntivo n. 848/03 emesso dal Tribunale di Cuneo sulla base della sola produzione di uno scambio di e.mail dalle quali si deduceva un riconoscimento di debito (e successivamente analogo decreto - decreto ingiuntivo n. 89/04 – è stato emesso dal Tribunale di Bari). E' seguito un animato dibattito tra chi sosteneva che l'e-mail dovesse ritenersi documento "scritto" idoneo a soddisfare i requisiti di cui agli artt. 633-634 c.p.c. e chi, invece, negava allo stesso documento qualsiasi valenza probatoria e formale. Si ricordano, da una parte, i contributi dottrinali di: V. AMENDOLAGINE, sempre a commento del decreto del Tribunale di Cuneo, dal titolo "*Il valore probatorio dell'e-mail nel ricorso per ingiunzione di pagamento*" apparso di recente su *Diritto e Giustizia on line*, Giuffrè editore, 2004, e dello stesso autore "*Dopo il Tribunale di Cuneo, anche quello di Bari si pronuncia a favore dell'accoglimento di un ricorso per ingiunzione di pagamento proposto sulla base di una ricognizione di debito trasmessa da una parte (creditore) all'altra (debitore) attraverso la posta elettronica*", su *Diritto e Giustizia on line*, Giuffrè Editore, 2004; S. CAMERINI, "*Provider e e-mail probatorie*", pubblicato dal *Consulente Legale Informatico* alla pagina http://www.consulentelegaleinformatico.it/approfondimentidett.asp?id=61; D. SCIALDONE, "*L'e-mail soddisfa il requisito legale della forma scritta?*", pubblicato su *Jei – Jus e Internet* alla pagina http://www.jei.it/infogiuridica/notizia.php?ID_articoli=306; F. SARZANA DI SANT'IPPOLITO, "*Firma elettronica e documenti contabili*", su *Punto Informatico* alla pagina http://punto-informatico.it/p.asp?i=46951; M. CUNIBERTI, "*E-mail e requisito di forma scritta*", pubblicato su *SCiNT* alla pagina http://www.scint.it/news_new.php?id=409; e ancora A. LISI, "*In giudizio una e-mail è valida?*", su *Punto Informatico* alla pagina http://punto-

dell'evoluzione e crisi della sottoscrizione autografa nel commercio internazionale e nel commercio internazionale elettronico.
Le contrattazioni moderne, infatti, da tempo utilizzano in maniera sempre più consueta *documenti dichiarativi non sottoscritti*, frutto delle innovazioni in campo "meccanico" o "telematico" (dal telegramma al telex, fino al telefax e alla *electronic mail*)([3]). Questo fenomeno globale imposto dagli scambi commerciali internazionali è stato più volte definito in dottrina come "crisi della sottoscrizione" e "aformalismo della macroeconomia" ([4]).
Con la "virtualizzazione" dell'accordo telematico il sistema tradizionale legato alla visione del documento - quale *res rappresentativa di un fatto* ([5]), imputabile giuridicamente attraverso la sottoscrizione – è entrato irrimediabilmente in crisi e si è pertanto reso indispensabile trovare nuove nozioni più elastiche di documento che tenessero conto delle innovazioni della prassi e rendessero giuridicamente ammissibili le moderne tecniche di attribuzione della paternità dello "scritto", prescindendo dai meccanismi tipici legati alla sottoscrizione. Si è arrivati, così, alle suggestive e "futuribili" conclusioni di chi si è spinto ad affermare che "il flusso degli elettroni nel computer è il nuovo inchiostro, i bits il nuovo alfabeto e la memoria della macchina la nuova carta" ([6]) o ancora che "la scrittura è un concetto ampio comprendente qualsiasi dichiarazione incorporata in un supporto materiale destinato a durare nel tempo. Non contano né il tipo di alfabeto né il tipo di supporto." ([7])
In questo modo, il *documento informatico* diventa *documento scritto,* a prescindere dal supporto che lo contiene.([8])

---

informatico.it/p.asp?i=46663; A. LISI, "*L'e-mail è forma scritta?*", su *Altalex* alla pagina http://www.altalex.it/index.php?idnot=250; A. LISI "*Essere o non essere: i moderni dubbi amletici di una e-mail anonima*", pubblicato su *Diritto&Diritti* alla pagina http://www.diritto.it/articoli/dir_tecnologie/lisi3.html. Dall'altra parte si ricordano i due scritti molto polemici di M. CAMMARATA e E. MACCARONE, "*Un messaggio e-mail non è* prova scritta", su *Interlex* alla pagina http://www.interlex.it/docdigit/provascritta.htm e "*Il diritto come guida, la tecnica come supporto*", sempre su *Interlex* alla pagina http://www.interlex.it/docdigit/provascritt2.htm. Meritano di essere ricordate le posizioni "intermedie" di coloro che attribuiscono un qualche valore di "documento informatico" all'e-mail, ma non di "documento firmato elettronicamente": L. DE GRAZIA, "*Firma Elettronica Non Avanzata. Una personale opinione sulla c.d.* firma elettronica debole", pubblicato su *Diritto&Diritti* alla pagina http://www.diritto.it/articoli/dir_tecnologie/firma_elettronica.pdf; G. ROGNETTA, "*E-mail e prova scritta secondo l'art. 10 Tuda*", pubblicato su *Diritto&Diritti* alla pagina http://www.diritto.it/articoli/dir_tecnologie/rognetta2.html.
([3]) Così D. RICCIARDI, Tesi di laurea, *Introduzione* a "*La cd. Firma Digitale*" pubblicata su *StudioCelentano*, alla pagina http://www.studiocelentano.it/publications_and_thesis/Ricciardi/index.htm.
([4]) N. IRTI, "*Idola libertatis*", Milano, 1985, 24 ss;
([5]) La definizione, come è noto, si deve a F. CARNELUTTI, "*La prova civile*", Padova, 1915, p. 184. Tale nozione è stata poi specificata in "cosa rappresentativa di un fatto giuridicamente rilevante", da L. CARRARO, "*Diritto sul documento*", Padova, 1941. In verità, il genio di CARNELUTTI si era già spinto oltre, arrivando ad ipotizzare l'irrilevanza della materia che costituisce il documento: "*qualunque materia, atta a formare una cosa rappresentativa può entrare nel documento: tela, cera, metallo, pietra e via dicendo*" (F. CARNELUTTI, in "*Novissimo dig. It.*", voce *Documento* (*teoria moderna*), p. 86. Adesso la teoria deve fare un passo oltre e, nell'abisso del vuoto immateriale fatto di *bit*, deve ipotizzare un documento informatico che prescinda dal suo supporto. Alcune norme ancora questo passo non l'hanno fatto (si veda, ad esempio, l'art. 491 bis del c.p.: "per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli"), mentre altre normative l'hanno fatto sino ad un certo punto, legando troppo lo sviluppo del documento informatico alle certezze del documento amministrativo (ovviamente si fa riferimento al D.P.R. 445/2000).
([6]) R. BORRUSO, "*Computer e diritto*", II, Milano, 1988, 218 ss.
([7]) E. GIANNANTONIO, "*Manuale di diritto dell'informatica*", Padova, 1997, 385.
([8]) *Così, diventano documenti scritti, secondo una nozione più ampia ed aggiornata di scrittura, non solo i documenti informatici in senso ampio, ma anche quelli in senso stretto. I secondi sono quelli conservati nella memoria dell'elaboratore e non possono essere resi manifesti se non attraverso la stessa macchina mostrando a video il testo o l'immagine o facendo ascoltare il suono riprodotto. Mentre i primi sono quelli formati dall'elaboratore attraverso i suoi dispositivi di output: stampante, video ecc.. Questi ultimi possono dunque essere resi su un supporto materiale - che può essere la carta della stampante, un microfilm ecc. - e, una volta formati, possono essere utilizzati senza l'ausilio della macchina*. Così G. RANA, "Il valore probatorio del documento elettronico", pubblicato su *Diritto&Diritti* alla pagina http://www.diritto.it/articoli/dir_tecnologie/rana.html#_ftn12.

"La parola dell'uomo deve viaggiare presto e lontano, e non può portare a lungo con sé il fardello della sottoscrizione autografa. La tecnologia fornisce mezzi sempre più semplici ed economici per realizzare questo fine: dapprima il telefax, poi i testi elaborati in forma digitale attraverso programmi che girano su personal computer e viaggiano con la posta elettronica ed Internet". ([9])
Ovviamente la parificazione di un documento informatico, come l'e-mail, alla "forma scritta" pone problemi innegabili e simili a quelli già noti relativi alla rilevanza formale e probatoria di telefax e telegramma o telex (profili probatori di avvenuta trasmissione e ricezione per il primo, mancanza di sottoscrizione per i secondi). ([10])
Problematiche queste che riguardano, quindi, i *profili probatori* di tali documenti e non la loro *natura formale* di "documento scritto" e che vengono a cadere e ad *evaporare* pressate dalle esigenze della pratica contrattuale internazionale e dell'aformalismo nella negoziazione tra privati. Problematiche che vanno risolte probabilmente in maniera diversa rispetto alle certezze dogmatiche della "tradizione" e cercando di tenere separati gli ambiti legati alle esigenze di "certificazione", tipici dei rapporti della P.A., da quelli dell'e-commerce internazionale. ([11]) L'orientamento comunitario e internazionale, infatti, è quello di liberare e svincolare il commercio elettronico e, quindi, i contraenti telematici dalle rigidità della firma digitale. ([12])

([9]) G. RANA, "*Il valore probatorio del documento elettronico*", pubblicato su *Diritto&Diritti* alla pagina già cit. . Così anche T. E. FROSINI, "*Telematica ed informatica giuridica*", in *Enc.del Dir*., XLIV, Milano, 1992, 60.
([10]) Così G. PASCUZZI, "*Il diritto nell'era digitale*", Bologna, 2002, p.79. Per un approfondimento si consiglia dello stesso PASCUZZI, "*Telex e telefax*", in *Digesto civ*., vol. XII, Torino, 1999.
([11]) Come già spiegato in altre occasioni, (A. LISI, *"In giudizio una e-mail è valida?",* già *cit.*) "ciò che ha un senso nei rapporti tra Pubbliche Amministrazioni e tra Pubbliche Amministrazioni e privati non necessariamente deve avere un senso nei rapporti 'più liberi' tra privati…" e ancora (sempre A. LISI, "*L'e-mail è forma scritta?*", su *Altalex*, già *cit.*) "occorre sempre ricordare che le esigenze del commercio, e soprattutto del commercio internazionale, sono certamente diverse dalle esigenze sottese ai rapporti che legano P.A. e cittadini. E infatti :
a) Tutte le norme che prevedono l'invio obbligatorio di e.mail con firma digitale riguardano particolari rapporti tra privati e pubbliche amministrazioni e, quindi, mirano a garantire maggiori esigenze di certezza dell'imputabilità e sicurezza del traffico telematico (dal 3 novembre 2003 la firma digitale è obbligatoria: per l'invio telematico degli atti societari ai registri camerali - DL 236/02 - DM 20/3/2003; dal 1.gennaio 2004 per l'invio della fattura 'europea' via e-mail - direttiva 2001/115/CE, art. 2; per le notificazioni dei trattamenti di dati personali al Garante – D.Lgv. 196/03, art. 38 ...).
b) Il T.U. 445/2000 è stato pensato per ricomprendere tutte le disposizioni legislative e regolamentari in materia di documentazione amministrativa: anche se contiene principi poi applicabili a privati ha questo 'vizio d'origine'.
c) La direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 sulle firme elettroniche è, invece, una direttiva che non pensava ad un unico quadro unitario per privati e pubbliche amministrazioni nell'utilizzo di sistemi che garantissero in qualche modo l'autenticazione e la sicurezza dei dati informatici trasmessi attraverso le reti telematiche (e, infatti, qui ritroviamo l'ampia definizione di firma elettronica leggera attuata dal nostro legislatore con il d.lgs. n. 10/2003 e mod. del 445/2000).
d) Nel d.lgs. n. 70/2003 (attuativo della direttiva 2000/31/CE), pensato, invece, per il solo commercio elettronico tra privati (e solo in via 'sussidiaria' per le P.A.), non si parla mai di firme elettroniche per la conclusione dei contratti e non si nega la validità di contratti conclusi e ricevuti via e.mail (basta leggere e confrontare - anche con ragionamento a contrario - gli articoli 12-13 del decreto).
Da ciò si deduce che manca in Italia un coordinamento tra le norme che regolano i rapporti tra PA e cittadino e le norme che regolano il mero commercio elettronico tra privati. Per il commercio elettronico tra privati non è necessario imporre sistemi di validazione e sicurezza identici a quelli indispensabili per i rapporti che si consumano con la PA."
Da ultimo, si segnala come nello stesso "Codice della privacy" (D.Lgs. 196/2003) si opera una importante differenza nella regolamentazione dei rapporti tra privati e rapporti cittadino-ente pubblico: infatti, mentre l'art. 9 specifica che la richiesta per l'esercizio dei propri diritti rivolta dall'interessato al trattamento di dati personali al titolare può essere effettuata "mediante lettera raccomandata, telefax o posta elettronica", invece la notificazione del titolare al Garante nei casi di cui all'art. 37 dello stesso Codice è validamente effettuata solo se trasmessa telematicamente, con firma digitale (ai sensi dell'art. 38). Si ricorda ancora che nel gennaio scorso è stata pubblicata sulla G.U. la Direttiva 27 novembre 2003 per l'utilizzo della posta elettronica nelle pubbliche amministrazioni, emanata dal Ministro per l'innovazione tecnologica di concerto con il Ministro per la funzione pubblica. Anche in questo caso, nei rapporti "interni" (che ci azzardiamo a definire "privatistici") della P.A. si consiglia l'utilizzo della posta elettronica, quale valido mezzo di trasmissione di documenti informatici, a prescindere da dissertazioni su firma elettronica o digitale.
([12]) Così G. ROGNETTA, "*Il consumatore tra point and click e firma digitale*", in *Commercio Elettronico e Tutela del Consumatore*, AA.VV., a cura di G. CASSANO, Milano, 2003, p. 203.

Una conferma a questo ragionamento la si ritrova nelle più sofisticate e importanti elaborazioni dottrinali in materia di contrattualistica comunitaria e internazionale: *The Principles Of European Contract Law 2002* ([13]) e *The UNIDROIT Principles of International Commercial Contracts* ([14]). I Principi UNIDROIT pubblicati nel 1994 e i Principi di diritto europeo dei contratti (PECL) possono essere considerati come il più prestigioso e riuscito "esperimento di codificazione" di un emergente regime giuridico sovranazionale e comunitario delle "transazioni" internazionali ([15]).
L'obiettivo è stato quello di individuare i principi comuni alla maggior parte dei sistemi giuridici esistenti e di elaborare una normativa *anazionale* applicabile ai contratti internazionali e comunitari "che potesse semplificare i rapporti giuridici che coinvolgono, per loro natura, più ordinamenti che spesso sono molto diversi fra loro". ([16])
I PECL e i Principi UNIDROIT sono stati elaborati quasi contemporaneamente da membri delle due commissioni di redazione in parte identici (in seno all'Unione Europea ([17]) e nell'ambito dell'UNIDROIT – *International Institute for the Unification of Private Law*) e le norme di cui gli uni e gli altri sono costituiti sono risultate in buona parte uguali nella sostanza: l'unica rilevante differenza è che mentre Principi Unidroit mirano a creare un quadro comune nella prassi commerciale internazionale (e sono molto utilizzati nella contrattazione internazionale e, quindi, ben conosciuti nei lodi arbitrali internazionali), i Principi PECL, invece, si rivolgono più genericamente ai contratti "civili". ([18])
Fatte queste dovute premesse sui PECL e sui Principi UNIDROIT, verifichiamo come questi prestigiosi regimi giuridici "anazionali" hanno risolto la particolare problematica della "forma scritta" nelle dichiarazioni contrattuali.
Nell'art. 1.10 *Definitions* dei Principi UNIDROIT si legge testualmente*: in these Principles "writing" means any mode of communication that preserves a record of the information contained therein and is capable of being reproduced in tangible form.* Quindi per "forma scritta" si intende *qualsiasi forma di comunicazione che conservi la documentazione delle informazioni contenute e*

([13]) Trattasi delle Parti I, II e III dei "THE PRINCIPLES OF EUROPEAN CONTRACT LAW 2002" (acquisibili sul web all'indirizzo http://www.jus.uio.no/lm/eu.contract.principles.parts.1.to.3.2002/toc). Per una traduzione in italiano effettuata con grande passione, accuratezza e precisione da C. CASTRONOVO si veda http://host.uniroma3.it/facolta/giur/materiale_didattico/elenco%20dispense/PRINCIPI.htm . Per approfondimenti si consiglia sempre di C. CASTRONOVO, "*Il contratto e l'idea di codificazione nei Principi di diritto europeo dei contratti*" in *Materiali e commenti sul nuovo diritto dei contratti* (a cura di G. VETTORI), Padova 1999, p.854-872 (*Italian version of Contract and the Idea of Codification in the Principles of European Contract Law*, in *Festskrift til Ole Lando*, Copenhagen 1997, p. 109-124) e "*I Principi di diritto europeo dei contratti e l'idea di codice"* in *Rivista del diritto commerciale e delle obbligazioni*, 1995, I, p. 21-38.
([14]) Acquisibili alla pagina web http://www.unidroit.org/english/principles/pr-main.htm. Per una traduzione in italiano si consiglia quella contenuta sul "*Manuale di diritto commerciale internazionale*" di F. BORTOLOTTI, Vol. 1, Padova, 2001, p. 909 e ss. E' scaricabile, inoltre, una traduzione in italiano dei Principi UNIDROIT all'indirizzo http://www.unidroit.org/english/principles/pr-main.htm. Per un breve approfondimento sui Principi Unidroit e sulla loro funzione nella prassi del diritto commerciale internazionale si consiglia la lettura di V. MASSARI, "*L'efficacia dei Principi Unidroit nella contrattualistica internazionale*" pubblicato su Diritto & Diritti cartaceo n. 10 Marzo 2002 e acquisibile alla pagina http://www.lapraticaforense.it/articolo.php?idart=100.
([15]) In verità, "I Principi non tendono ad essere applicati soltanto ai contratti internazionali. Gli articoli che li compongono sono principi generali del diritto dei contratti" (O. LANDO, "*Principles of European Contract Law. A First Step towards a European civil Code?*", in *Rev. dr. aff. int.* 1997, p. 196).
([16]) V. MASSARI, *op. cit.*
([17]) All'inizio degli anni ottanta una commissione, costituita su sollecitazione della Comunità europea e per iniziativa di OLE LANDO, professore alla Business School di Copenhagen, formata da insigni giuristi e professori dei vari Paesi della Comunità, ora Unione, europea, ha cominciato ad elaborare i *Princìpi di diritto europeo dei contratti e delle obbligazioni*.
([18]) "Benché con M.J. BONELL, *An International Restatement of Contracts Law*, Irvington, N.Y. 1994, p. 32, deve essere rilevato che per i Principi UNIDROIT la limitazione ai contratti commerciali non è intesa ad assumere la distinzione tradizionale in alcuni ordinamenti giuridici tra contraenti o contratti 'civili' e 'commerciali'; l'idea è, piuttosto, quella di escludere dall'ambito di applicazione dei Principi UNIDROIT i contratti dei consumatori" così C. CASTRONOVO, *Il contratto e l'idea di codificazione nei Principi di diritto europeo dei contratti*, cit., nota 15, p. 11.

sia riproducibile in forma tangibile. ([19]) Non si fa alcun cenno, quindi, alla sottoscrizione, in piena adesione a principi internazionali ormai universalmente riconosciuti e resi evidenti nella CONVENZIONE DI VIENNA SULLA VENDITA INTERNAZIONALE DI MERCI (Convenzione delle Nazioni Unite dell'11 aprile 1980), nella quale si includono nella nozione dello "scritto" tutte le comunicazioni, anche quelle a mezzo telegrafo e fax (art. 13 della Convenzione). Nel commento "ufficiale"([20]) ai Principi Unidrot, infatti, si legge "*a writing includes not only a telegram and a telex, but also any other mode of communication that preserves a record and can be reproduced in tangible form*". ([21])

Altrettanto espliciti sono i PECL, i quali all'art 1.301 (ex art. 1.105) - Meaning of Terms punto 6) espressamente affermano che *"written" statements include communications made by telegram, telex, telefax and electronic mail and other means of communication capable of providing a readable record of the statement on both sides*; anche in questo caso, la forma "scritta" si intende riferita ai telegrammi, telex, telefax, posta elettronica e ogni altro strumento di comunicazione in grado di produrre un documento suscettibile di lettura dall'una e dall'altra parte. ([22])

Ma come si possono piegare alle esigenze della prassi commerciale le tradizioni giuridiche basate sul documento cartaceo che "appartiene" da sempre ad un soggetto solo se da questi sottoscritto? Come già spiegato in altre occasioni ([23]), l'*appartenenza* del documento, cartaceo o informatico che sia, è stata individuata attraverso altri meccanismi, legati maggiormente all'innovazione tecnologica, a quel *senso di appartenenza nuovo* che si trova nel *potere di gestione dello strumento di trasmissione* ed è assolutamente slegato dalle ragioni di sicurezza e, quindi, di "evidenza probatoria" di quel documento (necessariamente affidata, quest'ultima al libero apprezzamento del giudice caso per caso).

Ci riportiamo ancora una volta alle parole di R. SACCO ([24]), per spiegare questo concetto: "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 cui si accompagna di norma un potere di fatto***"* ([25]).

Quindi, telegramma, telex, telefax, e-mail sono accumunati dal fatto di poter creare, in maniera, più o meno sicura, un *nuovo tipo di appartenenza* del documento al soggetto che l'ha redatto; in

---

([19]) Traduzione di F. BORTOLOTTI, *cit*, p. 910

([20]) Acquisibile alla pagina web http://www.unidroit.org/english/principles/chapter-1.htm .

([21]) Occorre riferire che dottrina e giurisprudenza sono già arrivate ad applicazioni elastiche e innovative del concetto di "forma scritta" associato all'evoluzione del documento informatico nel commercio elettronico B2C. Infatti, un'applicazione rigida delle normative a tutela del consumatore per i siti web B2C avrebbe in alcuni casi impedito la diffusione di questa nuova forma di commercio, rendendola illegittima. In particolare, si fa riferimento all'onere della "forma scritta" previsto per l'informativa di cui all'art. 5 del D. Lgs. 50/1992. Obbligo che renderebbe illegittima l'informativa semplicemente pubblicata in una pagina web. La legislazione successiva, avallando in parte gli orientamenti dottrinali (per tutti si cita G. SCORZA, *La tutela del consumatore in Internet*, Napoli, 2000, p.46) ha chiarito che "il consumatore deve ricevere conferma per iscritto o, a sua scelta, su altro supporto duraturo a sua disposizione ed a lui accessibile di tutte le informazioni" (art. 4 D.Lgs. 185/1999). Il passo logico successivo sarà quello di considerare pienamente legittima un'informativa fornita in maniera stabile e duratura in aree riservate e protette del sito web, previa autenticazione con *id* e *pw* del consumatore (poiché tale metodo di autenticazione può essere certamente considerato una forma di "firma elettronica leggera", equivalente della forma scritta).

([22]) Come da traduzione di C. CASTRONOVO, *cit*.

([23]) Ci si riporta per un approfondimento a quanto già scritto in "*Essere o non essere: i moderni dubbi amletici di una e-mail anonima*", *cit*. in nota 2.

([24]) Autore già citato in "*Essere o non essere: i moderni dubbi amletici di una e-mail anonima*", *cit*.

([25]) Dall'opera *Trattato di Diritto Privato* - diretto da P. RESCIGNO – *Vol. II Obbligazioni e Contratti* – ed. Utet 1982 p. 242.

qualche modo essi individuano il soggetto che aveva un potere di fatto, un controllo sullo strumento di trasmissione. ([26])
In questo senso tali documenti possono rientrare senz'altro nella categoria giuridica della "forma scritta", creando con l'autore dello "scritto", un legame nuovo, dettato da *nuove regole* scaturite dall'innovazione tecnologica e che, quindi, portano a "firmare" i documenti prescindendo, in particolari casi, dalla loro sottoscrizione.

***Segue*: L'e-mail è, quindi, "forma scritta"?**
"Nel lessico usuale si fa una certa confusione tra firma e sottoscrizione talché, a prima vista, non è dato con chiarezza scindere i concetti afferenti ai due vocaboli. Giuridicamente, invece, le differenze sono anche sostanziali, sicché si potrebbe affermare che la sottoscrizione sta alla firma come la *species* al *genus*, come la parte al tutto […] sottoscrivere vuol dire scrivere sotto, ossia letteralmente scrivere sotto uno scritto, un documento, un foglio, una qualsiasi scrittura quasi a sigillare i medesimi con l'impronta dei segni alfabetici formanti il nome, inteso nella sua più ampia accezione" (Dott. A. MORELLO, Voce *Sottoscrizione*, *Nuovissimo Digesto Italiano*, Torino, 1957)…la modernità di queste parole pur "*scritte*" ormai cinquant'anni fa è evidente, soprattutto perché attraverso le stesse si possono cogliere perfettamente anche le differenze tra *forma scritta* e *scrittura privata con sottoscrizione autografa*, tra *firma elettronica* e *firma digitale*, che tanto stanno facendo discutere in questi giorni...
La sottoscrizione conferisce la paternità al documento cartaceo, è il *suggello* della sua appartenenza ad un soggetto: su di essa si è sviluppata la tradizione giuridica dal diritto romano sino a qualche anno fa. Per alcuni atti e contratti la "forma scritta" viene richiesta *ad substantiam*, per altri *ad probationem*, per altri ancora, più importanti, è necessario l'atto pubblico (e, cioè, è necessario *suggellare* l'atto in presenza di un notaio) che attesti incontrovertibilmente la sua provenienza e riconoscibilità.
La semplice sottoscrizione cartacea per il nostro ordinamento (basato sull'*aformalismo* contrattuale) è, quindi, essenziale solo per alcuni atti e contratti (art. 1350 c.c. e altre fattispecie speciali previste dalla legge); essa, giova ricordarlo, non può ovviamente assicurare che il documento scritto e sottoscritto non sia stato modificato, alterato, o comunque che non provenga da colui che appare il suo sottoscrittore, salvo che ciò non sia riconosciuto in giudizio (o con un mancato disconoscimento o attraverso un esito positivo del procedimento di verificazione) (27). Occorre, quindi, ben differenziare gli aspetti probatori della "forma scritta", da quelli più "formali", previsti per la validità ed esistenza dell'atto.
Addirittura, già molti anni fa, il precedentemente citato MORELLO affermava "la dottrina sembra concorde nel ritenere che il documento esista anche se la sottoscrizione non sia conforme letteralmente alla norma (art. 6 cod. civ.) e sarebbe sempre possibile produrre in giudizio il contenuto di questa scrittura anche se priva di sottoscrizione, se attraverso un mezzo o una prova qualsiasi, si potesse accertarne la paternità, purché la stessa scrittura non sia richiesta *ad substantiam* per l'atto documentato"
Con queste essenziali premesse occorre rileggere le norme contenute nella direttiva 1999/93/CE - relativa ad un quadro comunitario per le firme elettroniche - e nel D.P.R. 445/2000 - Testo unico

([26]) Secondo una autorevole corrente dottrinale, il telefax dovrebbe coincidere solo e soltanto con una sorta di copia fotografica di un'altra scrittura, la quale potrebbe essere munita di sottoscrizione o meno e, quindi, esso avrebbe la stessa efficacia dell'originale, se la sua conformità non è disconosciuta o attestata da pubblico ufficiale (così S. PATTI, *Prova documentale*, in *Commentario del Codice civile Scialoja-Branca*, artt. 2699-2720, Bologna-Roma, 1996, pp. 151 s.). Ad avviso di chi scrive, invece, il telefax assume una sua autonomia funzionale nel momento in cui viene trasmesso, creando comunque quella "appartenenza" del documento, intrinseca nel potere di fatto che l'autore del documento ha con lo strumento di trasmissione utilizzato.
(27) Nel nostro ordinamento (artt. 2702 c.c. e ss) è, infatti, prevista la possibilità di poter disconoscere in giudizio la propria sottoscrizione negandone la paternità (quindi, eventualmente instaurare un procedimento per la verificazione della stessa…vd. artt. 214-215 c.p.c.)

delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - (come modificato in attuazione della stessa direttiva).
La "firma elettronica" (e anche la stessa "firma digitale") e la "sottoscrizione cartacea" sono ontologicamente diverse. Se la sottoscrizione cartacea assumeva sino a poco tempo fa valore determinante ed indispensabile per ricercare la paternità del documento ed assicurarne, in maniera più o meno sicura, la provenienza "incorporandosi" materialmente con lo stesso (senza comunque – lo ripetiamo ancora- assicurare con assoluta certezza la paternità e l'immodificabilità dello stesso), oggi la firma elettronica assolve funzioni simili in maniera ovviamente diversa.
La firma elettronica comporta necessariamente una "spersonalizzazione" del documento, prima legato fisicamente ad un soggetto attraverso la sottoscrizione ([28]): in passato era la *grafia* il criterio di collegamento, oggi è un *meccanismo informatico*! E i "meccanismi informatici" che legano in qualche modo il documento ad un soggetto possono essere tanti (dall'associazione di "id" e "pw" alla chiave biometrica): tutti più o meno sicuri nell'attribuire la paternità e la non modificabilità a quel documento ([29]). L'importante, quindi, non è assumere e verificare la sicurezza nella trasmissione con rigidi parametri informatici, ma semplicemente "parafrasare" e "aggiornare" un classico del diritto (R. SACCO, *cit.*) con le nuove scoperte tecnologiche: l'e-mail (prima era il telex) non dice con sicurezza chi ha inviato il messaggio, ma dice chi è l'utente…l'e-mail memorizza un messaggio, senza identificare (con certezza) il mittente. Il messaggio, però, identifica l'apparecchio trasmittente… La dichiarazione per e-mail individua il soggetto di un potere giuridico cui si accompagna di norma un potere di fatto e, più esattamente: *chi ha titolo per l'uso di questo strumento!*
Giustamente il legislatore comunitario ha, quindi, considerato - per quanto riguarda nello specifico il documento informatico - la categoria "firma elettronica cd. leggera" prescindendo dalla "tecnica" utilizzata per creare l'associazione del documento al suo titolare e questo con l'ovvia intenzione di lasciare libertà ai privati nel commercio elettronico (in modo che si possano trovare nel tempo anche nuove soluzioni tecnologiche più appropriate alle esigenze della prassi commerciale). In questo modo possono rientrare tra i documenti firmati elettronicamente tutti quei documenti che permettano, in maniera più o meno sicura, l'associazione del documento ad un soggetto: tra questi può certamente rientrare l'e-mail!
La firma elettronica *leggera* ha così una sua autonoma rilevanza rispetto alla firma digitale e non va confusa con la stessa: essa, pur non assicurando normalmente, con sicurezza paragonabile a quella della firma digitale ([30]), l'immodificabilità e la provenienza del documento, comunque permette di

---

([28]) Per un approfondimento si consiglia F. SARZANA DI SANT'IPPOLITO, *Il legislatore italiano e le firme elettroniche: la crisi del principio di unitarietà della sottoscrizione*, da "*Il Corriere Giuridico*" n.10/2003 - pg. 1375 ss. IPSOA e G. FINOCCHIARO, *Firma digitale e Firme elettroniche*, Milano, 2003, pg. 39 e ss.
([29]) Cfr. Commissione delle Comunità Europee, Proposta di direttiva del Parlamento Europeo e del Consiglio relativa a regole comuni sulle firme elettroniche, COM (1998) 297 def., par. I: "Esistono svariati metodi per firmare documenti in modo elettronico: da quelli molto semplici (ad esempio l'inserimento, in un documento realizzato con un programma di trattamento testi, dell'immagine ottenuta per scansione di una firma autografa) a quelli estremamente avanzati (ad esempio, le firme digitali che utilizzano la 'crittografia a chiave pubblica)". D'altronde, questa tesi (secondo la quale anche ID e PW possono in qualche modo rappresentare una forma di *autenticazione informatica* e, quindi, costituire una "firma elettronica") è stata già avallata da recente autorevole dottrina. Si veda, ad esempio, la posizione di A. GRAZIOSI, AA. VV. *Il documento informatico e la sua efficacia probatoria nel processo civile*, in un recente testo edito dalla Giappichelli, Torino, dal titolo *Commercio Elettronico Documento Informatico e Firma Digitale* a cura di C. ROSELLO, G. FINOCCHIARO E E. TOSI 2003 pg. 543; o ancora G. FINOCCHIARO, in *Firma digitale e Firme elettroniche, profili privatistici*, Milano, 2003, pg. 35 e ss. o il recente articolo di V. AMENDOLAGINE, sempre a commento del decreto del Tribunale di Cuneo, dal titolo "*Il valore probatorio dell'e-mail nel ricorso per ingiunzione di pagamento*" apparso di recente su *Diritto e Giustizia*, Giuffrè editore) o ancora G. VANGONE, "*Firme elettroniche*", La Nuova Giurisprudenza Civile Commentata" 4/2003, pubblicato anche alla pagina http://www.scint.it/appr_new.php?id=96 e, infine, da ultimo F. SARZANA DI SANT'IPPOLITO, *Firma elettronica e documenti contabili*, su Punto Informatico alla pagina http://punto-informatico.it/p.asp?i=46951.
([30]) Rimane da sottolineare, ancora una volta, che firma digitale e elettronica sono per loro natura diverse dalla sottoscrizione: "l'utilizzo del termine 'firma digitale', come pedissequa traduzione dell'inglese 'digital signature', appare potenzialmente foriero di pericolosi fraintendimenti, poiché dal punto di vista sistematico si tratta più di un

"associare" (o meglio attribuire) un documento ad un soggetto (nè più nè meno di un comune telefax o telex).In questo modo possono rientrare tra i *documenti firmati elettronicamente* tutti quei documenti che permettano, in maniera più o meno sicura, l'associazione del documento ad un soggetto: tra questi rientra certamente l'e-mail! E a questa fattispecie molto ampia di "firma elettronica leggera" (nella quale rientrerebbe anche l'e-mail) il legislatore ha voluto giustamente garantire un minimo di rilevanza giuridica (validità di "forma scritta" anche se liberamente valutabile dal giudice dal punto di vista probatorio) ([31]).
Insomma il necessario superamento del rigido formalismo previsto nella "forma scritta e sottoscritta" già si era verificato un bel po' di anni fa nella dottrina e giurisprudenza per strumenti nuovi quali telex, telefax, telegrammi e ora il problema si pone allo stesso modo per l'e-mail! E questo ragionamento è valido in tutti i casi in cui la "forma scritta e sottoscritta" non è prevista rigidamente per l'esistenza e validità dell'atto: con tale criterio logico l'e-mail, quale documento "firmato" (ma non sottoscritto), potrebbe (per fortuna) essere liberamente utilizzata nel commercio elettronico nazionale e internazionale, sia per tutti gli atti e contratti "a forma libera", sia anche in tutti quei casi dove si parla di "forma scritta" o "prova scritta", senza rigidamente collegarsi alla "forma scritta (e sottoscritta) per la validità ed esistenza dell'atto".
Si è già detto in precedenti articoli ([32]) dei vari casi in cui nel commercio elettronico (soprattutto B2B) è necessario e indispensabile (per ragioni pratiche e giuridiche) superare il rigido formalismo e dualismo "forma scritta"/"firma digitale". Si ricordano, a titolo di esempio: il caso di richiesta "prova scritta" in un procedimento sommario ([33]); il caso di "documentazione scritta o di consenso

---

'sigillo' che di una 'firma'" (così M CAMMARATA E E. MACCARONE, "*La firma digitale sicura*", Milano, 2003, p. 70). Il fatto di ritenere – giustamente - la firma digitale un "sigillo" ci fa percepire ancora di più il senso della nostra discussione, avvicinando questo strumento alla "certificazione pubblica" piuttosto che ai normali strumenti utilizzati negli scambi commerciali tra privati. Tutti i dubbi e le critiche feroci sollevati in merito al secondo comma dell'art. 10 del D.P.R. 445/2000 (come modificato dal D. Lgs. n. 10/2002) vengono meno se si considera che il legislatore, in questo caso, ha ritenuto di dover tenere separati il piano formale dal piano probatorio. Infatti, il legislatore attribuisce semplicemente al documento con firma elettronica *leggera* (o semplice) il valore della "forma scritta", ma non conferisce un valore preciso allo stesso dal punto di vista dell'efficacia probatoria (dovrà essere il giudice di volta in volta e in base alle circostanze concrete a valutare liberamente quel documento). Come già riferito, infatti, nel caso di documento cartaceo la presenza della sottoscrizione in calce al documento prova semplicemente la provenienza della dichiarazione, ma non la sua integrità e soprattutto autenticità e, cioè, la corrispondenza tra chi appare sottoscrittore e chi effettivamente l'ha sottoscritto (e, quindi, in pratica la corrispondenza tra colui che appare come autore della dichiarazione e chi effettivamente ne è stato l'autore). La prova dell'autenticità, potrà formarsi fuori dal processo tramite "autenticazione" ex art. 2703 c.c., o all'interno del processo tramite riconoscimento espresso o tacito della sottoscrizione (si ringrazia in proposito R. FERORELLI, per quest'ultima riflessione maturata in una vivace discussione in seno alla *Mailing List* del Centro Studi di Informatica Giuridica di Bari). La firma digitale, in verità, assicura un grado di sicurezza sulla provenienza e sulla non modificabilità del documento ben superiore rispetto ad una semplice sottoscrizione autografa. Sotto questo punto di vista è spiegabile (anche se pur sempre suscettibile di critica) la sua efficacia probatoria basata sulla "*piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto*", come previsto nell'articolo 10, 3° comma, del T.U.D.A.. Infine, la caratteristica della firma digitale di "incorporarsi" e, quindi, "appartenere" al documento (attraverso la cd. impronta di *hash*) legittima la sua possibile equiparazione alla scrittura privata con sottoscrizione autografa (come espressamente previsto, però, soltanto nel TUDA prima delle ultime modifiche normative).
([31]) A prescindere dalla nota distinzione tra forma *ad substantiam* e forma *ad probationem*, ormai la dottrina tende a prendere in considerazione la forma - o quale "esternazione" dell'atto e, cioè, caratterizzante il momento in cui l'atto si manifesta (contrapponendolo così al suo contenuto); - oppure quale requisito occasionalmente imposto circa le modalità attraverso le quali l'atto deve essere compiuto o circa il mezzo espressivo dal quale esso deve <<risultare>> (F. DI GIOVANNI – *La forma – in I Contratti in generale*, AA. VV., a cura di E. GABRIELLI – Utet, Torino, 1999, p. 768). Solo nel primo caso, quindi, la forma rimanda al paradigma generale dell'atto giuridico e si ravvisa una sua essenzialità costitutiva per lo stesso. Tale analisi andrebbe compiuta oggi alla luce delle nuove esigenze del commercio elettronico internazionale B2B.
([32]) "*In giudizio una e-mail è valida?"* su *Punto Informatico* alla pagina http://punto-informatico.it/p.asp?i=46663, "*L'e-mail in giudizio: approfondimento*" alla pagina http://punto-informatico.it/p.asp?i=46769 e, infine, "*Legittima la registrazione alla Personal Zone?*" all'indirizzo http://punto-informatico.it/p.asp?i=46020.
([33]) Dalla giurisprudenza dominante il telefax o il telegramma sono stati già riconosciuti valida "prova scritta" ai fini dell'emissione del decreto ingiuntivo: "tra i documenti considerati dall'art. 634 c.p.c. come prove "tipiche" rientrano le

scritto" per il trattamento dati personali; il caso della specifica approvazione per iscritto delle clausole vessatorie molto utilizzate nella contrattualistica internazionale, l'informativa "scritta" in favore del consumatore nel commercio elettronico B2C. In tutti questi casi, si deve operare una equiparazione del documento informatico con firma elettronica leggera (come l'e-mail) alla "forma scritta" (come già avvenuto nel caso del telefax, del telegramma, del telex), lasciando (necessariamente) massima libertà al giudice nella sostanziale valutazione probatoria di questo documento prodotto in giudizio.
La tecnologia galoppa e non possiamo certo pensare di bloccarla o di vincolarla soltanto all'utilizzo di alcuni strumenti (come la firma digitale), piuttosto che di altri.
Con questa legislazione italiana (ed europea) che commentiamo (da migliorare senz'altro) si è, quindi, cercato di contemperare le esigenze formali della P.A. con quelle più "pratiche" del commercio elettronico, e questo non è sempre facile o possibile…e <<in quest'ottica, mi pare vadano letti gli equilibrismi giuridici compiuti nel classificare come scatole cinesi i diversi sistemi di validazione informatica, partendo dalla firma elettronica pura e semplice, transitando per le figure intermedie della "firma elettronica avanzata" e della "firma elettronica qualificata", sino a giungere al modello italiano: la buona, vecchia "firma digitale">> ([34]).

***Segue:* Le altre conferme nella legislazione italiana e europea**
In verità - già prima delle contestate modifiche al DPR 445/2000 apportate con il Decreto legislativo 23 gennaio 2002, n. 10 (di attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche) - erano presenti nel nostro ordinamento normative penali che operavano una parificazione tra il documento informatico (quale l'e-mail) e il documento "scritto" (si pensi, ad esempio, ai già citati artt. 491 bis c.p. e 616 c.p.). Inoltre, da un punto di vista "contrattuale" (e, quindi, più vicino ai nostri scopi) nei rapporti di *subfornitura* (tipici rapporti B2B) una legge ha previsto espressamente questa parificazione (L. 192/1998 -"Disciplina della subfornitura nelle attività produttive" art. 2.1: "Il rapporto di subfornitura si instaura con il contratto, che deve essere stipulato in forma scritta a pena di nullità. Costituiscono forma scritta le comunicazioni degli atti di consenso alla conclusione o alla modificazione dei contratti effettuate per telefax o altra via telematica.").
Inoltre, si ricorda il Regolamento comunitario n. 41/2001 del 22 dicembre 2000 che, all' art. 23, II comma (in materia di clausole attributive della competenza), recita testualmente: "la forma scritta comprende qualsiasi comunicazione con mezzi elettronici che permetta una registrazione durevole della clausola attributiva di competenza".
Appare molto interessante rileggere in proposito alcune dichiarazioni contenute in un documento di lavoro sulla modifica dell'articolo 174 del regolamento (presentazione delle petizioni per posta elettronica), elaborato l'11 gennaio 2001 dalla Commissione Affari Costituzionali in seno al Parlamento Europeo (Relatore: Olivier Dupuis): " [..] Nella sostanza la posizione della Commissione per le petizioni è molto più "aperta" e garantisce a tutti i cittadini l'esercizio del diritto di petizione semplicemente attraverso l'invio di una e-mail (senza escludere le altre opzioni disponibili) o la compilazione del formulario presente nel sito internet del PE, e senza dover ricorrere al complesso meccanismo della firma elettronica avanzata. […] Essa dovrebbe inoltre dare la possibilità ai cittadini di depositare petizioni e firme (e-mail dei petenti con dati richiesti) per via elettronica e in particolare di aderire a petizioni già depositate inviando un semplice e-mail attraverso un software predisposto dal PE che permetta di farlo in modo semplice (ad esempio cliccando un bottone che apra un formulario dove inserire i propri dati di petente). La Commissione per gli affari costituzionali è dell'avviso che qualsiasi firma elettronica (sia essa semplice, come l'e-mail, o avanzata) possa essere riconosciuta come autentica, e che quindi il semplice invio di una

---

promesse unilaterali per scrittura privata, i telegrammi ed ora anche i telex e i fax" (C. App. Napoli 17.3.89; T. Ascoli 7.8.80; C. App. Ancona 5.4.82) e anche "le copie fotostatiche" (Tribunale Milano 3.1.85)…
([34]) M. PAPPALARDO, *Il recepimento della direttiva: in difesa del legislatore* , 03.07.03 su *Interlex* alla pagina http://www.interlex.it/docdigit/pappalardo.htm.

petizione per via elettronica sia sufficiente al fine del suo deposito, senza la necessità di un ulteriore invio cartaceo".
La tendenza legislativa e giurisprudenziale che accosta l'e-mail (e il documento informatico in genere) allo "scritto", nell'ottica delle dinamiche del nuovo linguaggio (sempre più oggi fatto di *bit*) e della stessa evoluzione giuridica del concetto di documento ([35]), appare addirittura ovvia ed inevitabile.
A volte, a rincorrere troppo la "tecnica informatica", si rischia di perdere di vista il senso di alcune innovazioni normative e di vincolare giuridicamente la prassi a rigide regolamentazioni che non tengono conto dei reali problemi del commercio e delle stesse ragioni dell'innovazione…
L'equiparazione della "forma scritta" al telefax e alla posta elettronica la ritroviamo (inaspettatamente) anche nella recentissima Direttiva CE "relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi", definitivamente approvata il 29.01.04 ([36]), laddove negli artt. 1 (definizioni) e 42 (regole applicabili alle comunicazioni) sono contenuti i principi fondamentali della disciplina delle nuove modalità di comunicazione: in tali articoli, si precisa preliminarmente che i termini "scritto" o "per iscritto" designano *un insieme di parole o cifre che può essere letto, riprodotto e poi comunicato e che può includere informazioni trasmesse e archiviate con mezzi elettronici, ossia con mezzi che utilizzano apparecchiature elettroniche di elaborazione (compresa la compressione numerica) e di archiviazione dei dati, tramite diffusione, trasmissione e ricezione via filo, via radio, attraverso mezzi ottici o altri mezzi elettromagnetici*. A fronte di un siffatto quadro definitorio l'articolo 42 prosegue affermando che "*tutte le comunicazioni e tutti gli scambi di informazioni di cui al presente titolo possono avvenire, a scelta dell'amministrazione aggiudicatrice, per posta, mediante fax o per via elettronica*".
Inoltre, come è noto, l'utilizzo della posta elettronica quale valido mezzo di trasmissione di documenti informatici era già previsto, in Italia, dall'art. 14 del Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (D.P.R. 445/2000); ma soprattutto occorre ricordare che il 27 novembre 2003 il Ministro Stanca ha emanato una Direttiva che prevede un utilizzo degli strumenti di posta elettronica per diverse attività "interne" della Pubblica Amministrazione (richieste di ferie o permessi, convocazioni di riunioni, invio di comunicazioni di servizio ovvero notizie dirette al singolo dipendente in materia di buoni pasto, pagamento di competenze, diffusione di circolari o ordini di servizio) ed, inoltre, il supporto, la formazione e l'assistenza alle P.A. per le iniziative relative alla revisione dei sistemi di comunicazione. ([37]).
Infine, a ulteriore conferma di quanto soprariferito, è di poche settimane fa la notizia che il Consiglio dei Ministri nella riunione del 25 marzo ha approvato uno schema di DPR ([38]), su

---

([35]) Il documento (da docere: insegnare, far conoscere) è, nel senso originario del termine, *qualche cosa che fa conoscere un fatto* (F. CARNELUTTI, *Definizione* del *Nuovissimo Digesto Italiano*, Torino, edizione 1957, diretta da A. AZARA E E. EULA p. 86), quindi è "qualche cosa" che rappresenta un fatto di rilievo giuridico. Con l'avvento dell'informatica quel legame indissolubile del documento con la cosa è venuto meno e, quindi, si è arrivati a definizioni più "moderne e tecnologiche" come quella di documento informatico contenuta nel tanto criticato Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 come modificato dal D.Lgs. 23 gennaio 2002, n. 10, dalla legge 16 gennaio 2003, n. 3 e dal DPR 7 aprile 2003, n.137): il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Alla luce di ciò l'e-mail - nel momento in cui rappresenta al suo interno atti, fatti o dati giuridicamente rilevanti, come una qualsiasi lettera, telefax, telegramma, fotografia etc. - è certamente un documento!
([36]) Direttiva C.E. 3 febbraio 2004 – (testo approvato dal Parlamento europeo il 29 gennaio 2004 e dal Consiglio il 3 febbraio 2004, non ancora pubblicato sulla GUCE – Dir. rif. 2000/0115 (COD), PE-CONS 3696/03). Testo acquisibile alla pagina http://www.lexitalia.it/leggi/direttivace_2004-02-03.htm.
([37]) Così M. IASELLI, "*L'e-mail assume valore legale? Non e' proprio così*", su StudioCelentano alla pagina http://www.studiocelentano.it/editorial/articolo.asp?id=899 .
([38]) Schema di decreto del Presidente della Repubblica recante regolamento concernente disposizioni per l'utilizzo della posta elettronica certificata (approvato dal Consiglio dei ministri del 25 marzo 2004). Acquisibile sul sito www.scint.it alla pagina http://www.scint.it/news_new.php?id=436. Per un primo commento dello schema di DPR si vedano gli

proposta di Lucio Stanca, Ministro per l'Innovazione e le Tecnologie, e Luigi Mazzella, Ministro per la Funzione Pubblica, che riconosce piena validità giuridica ai documenti trasmessi per posta elettronica: la posta elettronica può diventare "posta certificata", come una normale raccomandata con avviso di ricevimento, così che l'invio e la ricezione di documenti con strumenti informatici (e-mail) avrà "pieno valore legale". Inoltre, l'art. 16 dello schema di DPR prevede l'abrogazione del primo comma dell'art. 25 del DPR 445 del 2000, secondo il quale "in tutti i documenti informatici delle pubbliche amministrazioni la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente testo unico". Questa automatica sostituzione, pertanto, non sarebbe più prevista per legge e occorrerebbe fare una valutazione caso per caso circa lo strumento di comunicazione elettronica più opportuno da utilizzare per "digitalizzare" i documenti amministrativi... rimarrebbe in vigore soltanto il secondo comma dello stesso articolo secondo il quale "l'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti". ([39])
Secondo lo schema di DPR, quindi, l'e-mail "certificata" potrà essere liberamente utilizzata nei rapporti "interni" e di natura "privatistica" della P.A. e naturalmente nelle comunicazioni tra privati. Ovviamente, quando per taluni rapporti emergeranno esigenze di certezza e di "autenticazione" tipiche della P.A., allora serviranno altri meccanismi di "sigillazione" che possano assicurare il rispetto di quelle esigenze (come l'utilizzo della firma digitale o di altre forme di firma elettronica "avanzata" apposte sul messaggio).
Tale schema di DPR sembrerebbe, quindi, conferire ulteriore certezza al fatto che il legislatore italiano voglia uniformarsi alla tendenza comunitaria e internazionale che mira ad accostare l'e-mail ad altre forme di "documentazione scritta non sottoscritta" quali telefax, telegrammi, telex e, così, rafforzare ancora una volta le considerazioni intervenute in materia di valore dell'e-mail quale "forma scritta" (anche in seguito ai decreti ingiuntivi emessi dal Tribunale di Cuneo e Bari sulla base della produzione di e-mail contenenti un risconoscimento di un debito). ([40]).
Il legislatore comunitario e quello italiano sembrano confermare, pertanto, (anche per alcuni rapporti di natura "privatistica" tra P.A. e cittadino e/o impresa) una piena equiparazione formale tra comunicazione elettronica e comunicazione scritta: equivalenza formale che si ritrova più volte

---

articoli "*L'e-mail come una lettera raccomandata a.r.*" di A. LISI e M. IASELLI alla pagina http://www.scint.it/news_new.php?id=433 e "*Se la posta certificata sarà lettera raccomandata a.r., l'e-mail sarà posta ordinaria?*", di A. LISI alla pagina http://www.scint.it/appr_new.php?id=118.

([39]) Nella relazione illustrativa dello Schema di DPR si legge testualmente "L'articolo 16 dispone l'abrogazione dell'articolo 25, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2002, n. 445. La norma che si abroga ripropone, nel d.p.r. n. 445/2000, i contenuti dell'articolo 19 del d.p.r. 513 del 1997. Si tratta cioè di una disposizione introdotta in un momento in cui la firma digitale rappresentava l'unico strumento per la sottoscrizione informatica valido a tutti gli effetti di legge. La direttiva 1999/93/CE, recepita con il decreto legislativo 23 gennaio 2002, n. 10, ha invece previsto più tipologie di firme. In particolare l'articolo 10 del d.p.r. n. 445, nel quale sono confluite le modifiche di rango legislativo apportate con il citato decreto di recepimento, ha riconosciuto alla firma digitale valore analogo alla firma autografa (comma 2), ma ha anche riconosciuto che 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 (comma 3).
In tal modo è stata prevista una modalità di sottoscrizione che seppur non assimilabile alla firma autografa, ad essa può essere riconosciuta validità ad probationem. Alla luce di tale previsione, peraltro conforme al dettato comunitario non appare più necessario prevedere che in tutti i documenti delle pubbliche amministrazioni debba essere utilizzata la firma digitale. Con l'abrogazione dell'articolo 25 le pubbliche amministrazioni si regoleranno analogamente a tutti i soggetti dell'ordinamento applicando l'articolo 10 del d.p.r. n. 445/2000".

([40]) Ovviamente si deve attendere il testo definitivo del DPR per approfondire l'argomento e per verificarne il contenuto tecnico; in ogni caso da quanto riportato nel Comunicato Stampa del 22/03/2004 - pubblicato sul sito del Ministro per l'Innovazione e le Tecnologie alla pagina http://www.innovazione.gov.it/ita/comunicati/2004_03_25.shtml - tale DPR mira evidentemente ad attribuire un minimo di rilevanza giuridica ad uno strumento utilizzatissimo ed economico come l'e-mail! Dalla lettura del Comunicato, alla fin fine, non sembra che ci sia molta differenza "tecnica" tra la posta elettronica "certificata" e le "vecchie" e semplici e-mail e il tutto sembra essere un modo elegante per conferire rilevanza formale alla posta elettronica! I meccanismi tecnici di invio e ricezione sembrerebbero rimanere invariati, salvo le previste "ricevute di trasmissione".

ripetuta nell'ordinamento giuridico italiano, europeo, internazionale nel momento in cui si è voluta accostare l'e-mail al telefax, al telegramma, al telex…

***Segue:* E-mail, documento informatico e firme elettroniche leggere**

Dopo tutte queste lunghe premesse, si spera che possano essere più chiare alcune affermazioni che qui di seguito si specificano e ribadiscono.

Eviteremo di ripetere quanto già detto da altri autori circa la complessa "gradazione probatoria" in materia di firme elettroniche che il legislatore italiano ha previsto con la nuova normativa (per tutti si veda F. SARZANA DI SANT'IPPOLITO - Profili giuridici delle firme elettroniche - su Punto Informatico alla pagina http://punto-informatico.it/p.asp?i=46847). Come ampiamente riferito dall' autore testè citato (e in perfetta sintonia con quanto detto in questi giorni) <<l'impostazione di fondo della nuova disciplina è quella della liberalizzazione e semplificazione dell'uso delle firme elettroniche ed il riconoscimento della validità anche a firme "semplici", dotate cioè di uno standard tecnico più blando e che non sono perfettamente idonee, come avviene nel caso della firma digitale, a soddisfare le esigenze di integrità, segretezza, imputabilità e non ripudiabilità della sottoscrizione.

A termini del nuovo regolamento non può essere, infatti, negata rilevanza giuridica né ammissibilità come mezzo di prova alle firme elettroniche semplici o deboli, le quali si differenziano da quelle avanzate o forti per un diverso livello di sicurezza correlato al meccanismo di formazione e certificazione, e per una diversa efficacia giuridica del documento su cui sono apposte. Le ragioni di una modifica così radicale, attuata per seguire i principi comunitari, risiedono a monte da un lato nella diversa "sensibilità" comunitaria rispetto al tema della espansione del commercio elettronico e dall'altro nella consapevolezza della Commissione Europea di dover utilizzare strumenti normativi tecnologicamente "neutri" […] il Legislatore comunitario, come già avvenuto in passato nel settore della Società dell'Informazione, ha ritenuto di dover assumere un atteggiamento "neutrale" rispetto alle soluzioni tecnologiche, per non sviluppare logiche di mercato anticoncorrenziali e per lasciare aperta la porta ad una futura evoluzione tecnologica difforme>>.

La firma elettronica cd. "debole", è (come già più volte detto) definita, in maniera volutamente generica, come *l'insieme dei 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). Per la firma elettronica leggera non sono previsti dal legislatore *sistemi di validazione e di certificazione* (necessari, invece, per le firme elettroniche avanzate) ([41]). I cd. *metodi di autenticazione informatica* ([42]) sono invece genericamente *tutto quell'insieme di strumenti elettronici e delle procedure per la verifica indiretta dell'identità*, secondo la definizione fornita dal D.Lgs. 196/2003 all'art. 4 comma 3 lett. c) - quali ad esempio, l'uso di password o di codici di identificazione personale, così come qualsiasi altro metodo che permetta in maniera diretta (o indiretta) un'identificazione (a prescindere da qualsiasi valutazione sulla sicurezza di quella

([41]) Così G. FINOCCHIARO già cit. p. 120.

([42]) Si è sostenuto – senza dimostrarlo – che il termine *autenticazione* utilizzato dal nostro legislatore sarebbe il risultato di un'erronea traduzione dell'inglese, in quanto il termine *authentication* significherebbe *validazione*! E' curioso che il legislatore quando parla di firma digitale *traduca* bene il termine "validazione" e quando parla di firma elettronica, no, e poi si sia sbagliato ad utilizzare questo termine anche in una legge successiva sul trattamento dei dati personali (D.Lgs 196/2003)! Si crede che il legislatore possa a volte sbagliare, ma che sia così "smemorato" sembra veramente inverosimile… In ogni caso, in mancanza di altri riferimenti concreti ci si deve ovviamente attenere al significato letterale delle parole (in italiano). Comunque chiediamo all'autore dell'articolo (M. CAMMARATA, *cit.*) di rivelare quale particolare dizionario inglese-italiano possiede visto che vari dizionari utilizzati riportano il termine *authentication* come sinonimo di *autenticazione* (Dizionario Inglese Italiano Ragazzini, 1967 ; Dizionario Inglese – Italiano Borelli – Chinol – Frank 1977; Dizionario Inglese – Italiano Collins 2000). In ogni caso, il significato "tecnico" e generalmente accettato di sistemi di *authentication* per le firme elettroniche è: "A technical definition of authentication is the process of establishing whether someone or something is who or what its identifier states it is. An authentication process may be enabled by:

-something you know, like a PIN or password;

-something you have, as with smartcards, challenge-response mechanisms, or public-key certificates;

-something you are, as with positive photo identification, fingerprints, and biometrics".

identificazione, perché tali valutazioni riguardano il profilo probatorio e sono, quindi, affidate al prudente apprezzamento del giudice).
Per una e-mail, quindi, l'inserimento "*a monte"* di identificativi quali ID e PW *associati* agli *headers* presenti nel messaggio *associati* alla stessa "firma" in calce al documento *associata* all'indirizzo e.mail conosciuto, certamente costituiscono una forma (sia pur leggera) di firma elettronica.
L'e-mail, si ripete ancora, pur non assicurando, con sicurezza paragonabile alla firma digitale, l'immodificabilità e la provenienza del documento, comunque permette di attribuire (e, quindi, "firmare") un documento ad un soggetto (nè più nè meno di un comune telefax o telex): l'autenticazione informatica non garantisce (perché la legge non lo richiede) l'immodificabilità e l'integrità del documento, né la sua sicura provenienza. Con tale normativa il legislatore mira, pertanto, a garantire un minimo di rilevanza giuridica formale a tutti questi "flussi documentali" (spesso internazionali) così diffusi nella prassi commerciale (a differenza della firma digitale che ancora stenta a decollare)([43]).
Un'ultima osservazione per concludere il nostro lungo discorso: voler considerare l'e-mail come una semplice "riproduzione meccanica" comporterebbe un evidente contrasto con la sua natura; infatti, l'e-mail ontologicamente non è la copia di qualcos'altro, ma è un originale ([44])…
In verità, come ben espresso da T. BALLARINO (in *Introduzione* al *Trattato breve di diritto della Rete* diretto da A. SIROTTI GAUDENZI, Rimini, 2001) "nel commercio elettronico, i giuristi di oggi devono compiere in pochi anni e sotto la pressione delle esigenze quotidiane un'opera di revisione e riconversione dell'ordinamento giuridico nel suo insieme non dissimile da quella che fu fatta a suo tempo per adeguare il diritto romano e imperiale – statico per origine e vocazione – alle esigenze di un mondo che aveva "scoperto" gli strumenti per progredire. (…) Il compito del giurista, oggi, è di adattare il fenomeno Internet alle regolamentazioni statali che sopravvivono". E allora ogni "cybergiurista", se ha in mente realmente di risolvere le problematiche pratiche della prassi telematica, dovrebbe prima di tutto chiudere gli occhi e "dimenticare" le proprie certezze

([43]) In questo saggio si evita di addentrarsi in difficili valutazioni tecniche circa la sicurezza dell'e-mail nel "procedimento di autenticazione". Si ripete comunque che tali valutazioni esulano dai compiti del giurista, il quale deve semplicemente *sussumere* (come hanno fatto i giudici con i decreti ingiuntivi emessi sulla base di un riconoscimento di debito via e-mail) *un caso concreto in una fattispecie astratta prevista dalla legge*, basandosi eventualmente su valutazioni legate alla prassi. In ogni caso, parlare di *autenticazione informatica* per sistemi di trasmissione molto diversi tra loro quali i sistemi di trasmissione delle e-mail (webmail o con client di posta o reti private) significa anche andare al di là di quelle che sono state le stesse intenzioni del legislatore, nel momento in cui ha voluto inserire nel nostro ordinamento un *genus* di firma che racchiudesse sistemi di autenticazione tra loro diversi (diversi anche dalle e.mail, come i sistemi di ID e PW per l'accesso all'area riservata di un e-marketplace), affidando così al giudice la valutazione caso per caso. E' stato eccepito, in proposito, che spesso (ma non sempre, e si sta comunque iniziando ad andare *tecnicamente* in senso contrario, come anche dimostrato dallo sviluppo e dalla regolamentazione di servizi di "posta elettronica certificata") il server *smtp* utilizzato per l'invio del messaggio non effettua un'autenticazione *in uscita*, mentre *in entrata* ovviamente questa autenticazione si ha sempre tramite (generalmente) POP3. Si sottolinea, comunque, che le trattative commerciali sono frutto di una lunga fase precontrattuale e, quindi, nei vari scambi forme di autenticazione *in entrata* ci sarebbero sempre. E' stato ancora eccepito che nell'e-mail l'autenticazione non è effettuata sul documento, ma semplicemente dal servizio che individua un pc…ciò è ininfluente perché la stessa problematica è insita nel telex o nel telefax o nel telegramma e, come già riferito, si parla di *firma* non di *sottoscrizione*. Ci si riporta ancora una volta alla dottrina tradizionale (R. Sacco citato) per ribadire che "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 cui accompagna di norma un potere di fatto". Stessa cosa avviene con le e.mail dove generalmente tramite *headers* e *numero IP* si riesce a risalire facilmente al pc utilizzato da colui che ha sottoscritto un contratto con un ISP (e si "*autentica*" con un sistema di IP e PW..)…ma, ripetiamo, gli aspetti della sicurezza nell'autenticazione sono assolutamente ininfluenti e rimessi al prudente apprezzamento del giudice. Infine, occorre ricordare che la normativa in materia di trattamento dei dati personali comporterà sempre di più l'attento utilizzo del proprio sistema informatico "legato" al suo utilizzatore/titolare tramite un sicuro sistema di autenticazione.
([44]) La versione stampata dell'e-mail, invece, coinciderebbe ovviamente con una "riproduzione meccanica" (cfr. C. M. BIANCA *Diritto Civile – Volume 3: Il Contratto* - Milano 2000 p. 309-310).

dogmatiche sedimentatesi sulla sottoscrizione cartacea e, quindi, procedere ad una lenta difficile revisione dei vecchi schemi mentali e ad una rivisitazione del diritto nell'ottica dello schermo del computer attraverso il quale in pochi attimi e con la pressione di pochi tasti negoziali virtuali sta appena acquistando un volume giuridico…

Con il presente saggio, quindi, si mira a sottolineare come sia necessario per il legislatore e per il giurista, conferire rilevanza alle prassi realmente in uso nel commercio elettronico, al fine di evitare di costringere alcuni protagonisti dell'e-commerce a continuare a far viaggiare i loro interessi in zone d'ombra non regolamentate o, meglio, non "legittimate" giuridicamente: dai semplici invii di auguri, alle proposte contrattuali e precontrattuali inviate via e-mail, sino alle transazioni commerciali nelle aree riservate di siti di *e-marketplaces*, miliardi di bit trasmettono una mole sconfinata di informazioni che rischiano di rimanere isolate nel limbo del "quasi giuridico".