CONSIGLIO NAZIONALE
DEI DOTTORI COMMERCIALISTI

FONDAZIONE
ARISTEIA
ISTITUTO DI RICERCA
DEI DOTTORI
COMMERCIALISTI

DOCUMENTI ARISTEIA

documento n. 2

La firma digitale nella previsione del d.p.r. 445/'00

maggio 2001

LA FIRMA DIGITALE NELLA PREVISIONE DEL D.P.R. 445/’00

DOCUMENTO ARISTEIA N. 2

LA FIRMA DIGITALE NELLA PREVISIONE DEL D.P.R. 445/'00

SOMMARIO: 1. Introduzione - 2. Cenni sul commercio elettronico - 3. La firma digitale - 4. La firma digitale nella previsione del d.p.r. 445/'00 - 5. La certificazione delle chiavi e gli enti certificatori - 6. Efficacia probatoria - 7. La firma digitale autenticata e l'atto pubblico.

1. INTRODUZIONE

Il rapido ed inarrestabile sviluppo di Internet, cui abbiamo assistito nel corso degli ultimi anni, ed il relativo moltiplicarsi di utenti e di servizi *on-line* hanno generato una nuova tipologia di scambi: quella telematica.

Attraverso il processo di globalizzazione dei mercati, inteso come abbattimento delle barriere fisiche e conseguente libertà di accesso agli scambi grazie alla smaterializzazione dei medesimi, il recente sviluppo della *new economy* e dell'*e-commerce* ha comportato dirette ed inevitabili conseguenze sul piano giuridico.

A fronte del dilagante fenomeno, il problema sostanziale consiste nello studio dell'eventuale compatibilità della normativa che regola l'interscambio tradizionale con le nuove metodologie telematiche, attraverso una analisi interpretativa che, partendo dalla *ratio* degli istituti tradizionali, tenga soprattutto conto della complessità della realtà fattuale di Internet.

Se da un lato è inevitabile ed inarrestabile lo scambio telematico, dall'altro è altrettanto inevitabile ed indispensabile stabilire i canoni ed i limiti che attribuiscano valore giuridico a detto scambio, nonché garantire la riservatezza e l'integrità del medesimo.

In tal senso, elemento di svolta in Italia è stata l'emanazione della legge n. 59 del 15 marzo 1997 (Legge c.d. Bassanini), il cui art. 15 ha attribuito rilevanza e validità giuridica - a tutti gli effetti di legge - agli atti, ai dati ed ai documenti della pubblica amministrazione e dei privati formati con strumenti informatici o telematici ed ai contratti stipulati nelle medesime forme, ed alla loro archiviazione e trasmissione per il mezzo di strumenti informatici. Detta legge ha, inoltre, disposto

l'emanazione, entro centottanta giorni, di specifici regolamenti atti a fissare i criteri e le modalità di applicazione dell'art. 15 in questione. Il regolamento di attuazione della norma, emanato il 10 novembre 1997 con decreto del Presidente della Repubblica n. 513 (pubblicato sulla Gazzetta Ufficiale del 13 marzo 1998) - e seguìto dal decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999 con il quale sono state fissate le regole tecniche per la formazione e divulgazione dei documenti informatici - all'art. 2 ribadisce la rilevanza del documento informatico conforme alle disposizioni del regolamento medesimo, a tutti gli effetti di legge, ed all'art. 4 specifica come detto documento, in quanto munito dei requisiti previsti dal regolamento, soddisfi il requisito legale della forma scritta.

Il regolamento attuativo 513/'97 è stato recentemente abrogato ed inglobato nel Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, emanato il 28 dicembre 2000 con decreto del Presidente della Repubblica n. 445 (pubblicato sulla Gazzetta Ufficiale del 20 febbraio 2001), che ha riordinato la normativa in materia di firma digitale, documentazione elettronica ed amministrativa, sulla base dei principi indicati dalla l. 8 marzo 1999, n.50 sulla predisposizione dei Testi Unici. L'art. 2 del d.p.r. 445/'00, in conformità con il II comma dell'art. 15 della l. 59/1997, specifica che le norme concernenti i documenti informatici e la firma digitale si applicano anche nei rapporti tra privati. Le regole tecniche di cui al d.p.c.m. 8 febbraio 1999, non sono state abrogate dal d.p.r. 445/'00; ai sensi della lettera f) dell'art. 78 del d.p.r. (rubricato sotto la dizione "norme che rimangono in vigore"), infatti, "fino alla loro sostituzione, i regolamenti ministeriali, le direttive e i decreti ministeriali a contenuto generale, nonché le regole tecniche già emanate alla data di entrata in vigore del presente Testo Unico", restano comunque in vigore (la normativa è reperibile al sito dell'AIPA - Autorità per l'Informatica nella Pubblica Amministrazione - www.aipa.it).

2. CENNI SUL COMMERCIO ELETTRONICO

In merito al riconoscimento della validità del contratto concluso per via telematica o con strumenti informatici, è intervenuto il d.p.r. 513/'97, il cui art. 11, (successivamente recepito nel Testo Unico 445/'00 all'art. 11), prevedendo che detti contratti stipulati mediante l'uso della firma digitale sono validi e rilevanti a tutti gli effetti di legge e che ad essi si applicano le disposizioni vigenti in materia di contratti negoziati al di fuori dei locali commerciali (di cui al decreto legislativo 15 gennaio 1992, n. 50), ne ha sancito la validità. Detto riconoscimento comporta però la verifica della compatibilità della normativa civilistica in ordine alla formazione ed alla conclusione del contratto.

Se per il caso in cui il computer venga adoperato per la sola trasmissione delle dichiarazioni di volontà via e-mail non sorgono particolari difficoltà interpretative, qualora il supporto informatico sia a fondamento del contratto stesso, come per il caso di contratti via Internet, è necessario analizzare il meccanismo di formazione negoziale.

Il contratto, come definito all'art. 1321 c.c., è l'accordo di due o più parti volto a costituire, regolare o estinguere tra loro un rapporto giuridico di natura patrimoniale. L'accordo tra le parti, ossia l'incontro delle volontà espresso attraverso l'alternanza della proposta e dell'accettazione, oltre ad essere il primo degli elementi essenziali del contratto *ex* art. 1325 c.c., è il fulcro stesso del medesimo ed in tal senso il contratto è concluso quando il proponente ha conoscenza dell'accettazione dell'altra parte.

Nella contrattazione telematica, tanto le modalità attraverso cui si propongono i servizi e i beni on line, quanto la manifestazione della volontà contrattuale, si esprimono in modo del tutto analogo rispetto alle negoziazioni tradizionali.

Il sito commerciale viene paragonato ad una vetrina virtuale contenente l'offerta di beni e/o servizi e dunque tutti gli elementi di una qualunque proposta contrattuale intesa come offerta al pubblico; proposta che viene accettata attraverso l'esternazione della volontà dell'oblato che si rende manifesta o con il cosiddetto point and click (ossia ciccando sul tasto "per accettazione"), ovvero con la digitazione del numero della carta di credito. Per il caso in cui, invece, manchino alcuni degli elementi contrattuali (ad esempio l'oggetto non è determinato nella sua interezza ovvero non è espresso il prezzo di ogni singolo articolo, ma solo il prezzo massimo ed il minimo rispetto alla pluralità di oggetti offerti), non potendosi parlare di offerta al pubblico, si prospetta la fattispecie dell'invito a proporre, ossia l'invito alla trattativa vera e propria formata dall'offerta e della controfferta.

Aderendo ad un autorevole dottrina, entrambi i casi danno modo di argomentare a favore della natura negoziale dell'atto conclusivo dell'accordo, informata sulla disponibilità per le parti di stabilire gli effetti dell'atto stesso. Nel primo caso si avrà una negoziazione tacita dei contenuti contrattuali che verranno accettati così come proposti dal proponente, mentre nell'ipotesi di invito a proporre si aprirà una completa trattativa negoziale.

Quanto sinora detto porta ad escludere l'ipotesi prospettata da parte della dottrina di configurare la trattazione telematica non come accordo contrattuale ma come atti unilaterali distinti, l'uno di proposta e l'altro di accettazione, che non possono essere ricondotti a momenti contrattuali per la mancanza della negoziazione tra le parti.

Per quel che riguarda la conclusione del contratto, ai sensi dell'art. 1326 c.c., precedentemente citato, il contratto si ritiene concluso al momento in cui la parte proponente viene a conoscenza

dell'accettazione della controparte. Sia per il caso in cui si proceda all'accettazione tramite point and click, sia tramite digitazione del numero di carta di credito, la digitazione medesima, come la "cliccata", costituisce inizio dell'esecuzione della prestazione contrattuale *ex* art. 1326 c.c., e dunque il contratto inizia a spiegare i propri effetti. Lo stabilire il momento di conclusione ed inizio dell'esecuzione del contratto ha rilevanza al fine di determinare la responsabilità per inadempimento degli obblighi contrattuali. In tal senso, nel corso degli atti preparatori, ossia dell'incontro delle volontà fino al momento della conclusione del contratto, le parti rispondono per *culpa in contrahendo*, sottostando ad un regime di responsabilità precontrattuale, mentre dal momento della conclusione del contratto, anche per il caso in cui l'esecuzione del medesimo sia differita nel tempo, il mancato adempimento degli obblighi nascenti dal contratto comporterà responsabilità contrattuale *ex* art. 1218 c.c. La responsabilità precontrattuale comporta il risarcimento del danno da illecito civile e dunque soggiace al regime dell'onere probatorio di cui all'art. 2043 c.c.; colui che ritiene di aver subito il danno ingiusto sarà tenuto a provare che detto danno è stato a lui prodotto dall'azione o omissione di colui che ritiene responsabile. Al contrario, la responsabilità contrattuale comporta l'inversione dell'onere probatorio, ossia non è colui che ha subito il danno a dover dimostrare il mancato adempimento della controparte, bensì ai sensi dell'art. 1218 c.c., il debitore è ritenuto direttamente responsabile della mancata esecuzione della prestazione oggetto del rapporto obbligatorio; la parte non inadempiente sarà tenuta solamente a dimostrare l'esistenza del credito.

Inoltre, un ulteriore aspetto che incide sulla determinazione del momento di conclusione e di esecuzione del contratto riguarda il diritto di recesso.

Detto diritto, previsto all'art. 9 del decreto legislativo n. 50 del 15 febbraio 1992 per i contratti stipulati al di fuori dei locali commerciali e dunque anche per i contratti conclusi per via telematica o con strumenti informatici, è posto a tutela del consumatore e, da un lato, consente unilateralmente al consumatore di recedere dal contratto sottraendosi alle conseguenze giuridiche dello stesso mentre, dall'altro, impone l'obbligo di una adeguata informazione in merito al diritto stesso. In tal senso, il decreto legislativo n. 185 del 22 maggio 1999 sui contratti a distanza, in attuazione della direttiva comunitaria 99/7/CE, limita ai rapporti contrattuali tra *business* e *consumer* l'applicazione delle norme a tutela del consumatore (escludendo una tutela analoga per i rapporti *business to business*); norme che prevedono una adeguata informazione circa i principali elementi del contratto, circa i costi della transazione telematica e circa l'esistenza del diritto di recesso.

Il consumatore, una volta ricevute dette informazioni in tempo utile prima della conclusione del contratto, è tenuto a confermarle per iscritto al più tardi al momento dell'esecuzione del contratto.

In ultima analisi, le eventuali clausole vessatorie (ossia quelle clausole che stabiliscono a favore di chi le predispone limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti con i terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziale) inserite nel contratto, ai sensi del II comma dell'art. 1341 c.c., dovendo essere approvate per iscritto per avere effetto, comportavano la necessità di ripetere per iscritto il contratto telematico al fine di sottoscriverle; mentre, con la firma digitale, il problema può dirsi ovviato, in quanto è possibile approvarle on line sottoscrivendole digitalmente.

3. LA FIRMA DIGITALE

In tema di riconoscimento giuridico della validità delle transazioni telematiche, assume rilevanza la difficoltà di garantire l'integrità e la riservatezza dei documenti e degli scambi, nonché la paternità delle azioni svolte in rete.

Internet è un canale "non sicuro". Essendo una rete di interconnessione, necessariamente interconnette l'intero universo di utenti e poiché ogni azione compiuta in rete lascia tracce "astrattamente" ripercorribili, ogni transazione può essere soggetta ad atti di pirateria informatica, nonché a monitoraggi non desiderati; ma non solo, essendo la comunicazione in Internet indiretta e mediata dal supporto informatico ed essendo assai frequente l'uso di pseudonimi o di misure elusive, risulta estremamente difficile, da un lato, avere la certezza della controparte con cui si sta operando e, dall'altro, attribuire, con un discreto margine di sicurezza, la paternità degli atti compiuti ai legittimi "padri".

Nasce così l'esigenza di trovare degli strumenti idonei a conferire il connotato di giuridicità agli interscambi telematici.

L'art. 1 del d.p.r. 445/'00 è dedicato alla definizione del documento informatico e dei suoi elementi, mentre alla sezione V del capo II viene disciplinata la firma digitale e la certificazione della stessa.

La previsione della firma digitale e della sua disciplina, trova la sua radice di giustificazione, sia nella necessaria tutela della riservatezza e dell'integrità delle transazioni, sia nella esigenza giuridica della sottoscrizione, intesa come metodologia volta a garantire la paternità di un documento (fino ad oggi - di norma - cartaceo) al fine di attribuirgli rilevanza giuridica. Tradizionalmente, infatti, lo scopo

dell'apposizione autografa e leggibile del nome e del cognome in calce al documento cartaceo è sempre stato quello di supplire alle tre funzioni tipiche della sottoscrizione, ossia la funzione indicativa, tesa per l'appunto ad identificare l'autore, la funzione dichiarativa, che comporta il riconoscimento di paternità da parte del sottoscrittore medesimo, e la funzione probatoria.

Per avere rilevanza giuridica, dunque, anche il documento informatico doveva rispettare necessariamente il requisito della sottoscrizione, al fine di assicurare la paternità dell'atto e quindi l'assunzione di responsabilità dell'autore riguardo agli effetti che da esso discendono.

In tal senso, secondo la previsione dell'art. 10 del d.p.r. 445/'00 (*infra* § 5), combinato con il disposto di cui all'art. 1 e con particolare riferimento alla lettera n), l'apposizione della firma digitale al documento informatico, garantendo la soddisfazione del requisito legale della forma scritta, attribuisce validità e rilevanza giuridica - a tutti gli effetti di legge - al medesimo documento così formato, come previsto all'art. 8 del sopra citato regolamento.

Ma la firma digitale, ancorché idonea a soddisfare il requisito della forma scritta supplendo alle tre funzioni della sottoscrizione ed ancorché equiparabile alla sottoscrizione autografa tradizionale, va da quest'ultima comunque distinta. In tal senso, basti pensare ai requisiti tipici della sottoscrizione, ossia l'autografia, la leggibilità e la nominatività; nessuno di essi è direttamente riscontrabile nella firma digitale e ciò in quanto essa è digitata e non scritta di pugno dal titolare, è illeggibile se non attraverso la chiave di decifratura ed è composta da una sequenza di caratteri alfanumerici anziché dal nome del titolare.

Ciò detto, al fine di comprendere meglio l'equiparabilità della firma digitale alla sottoscrizione, nonché la portata dei testé citati articoli, si avverte la necessità di chiarire il significato della firma digitale attraverso l'analisi del sistema di chiavi asimmetriche previsto dal regolamento.

La firma digitale, dopo essere definita alla lettera n) dell'art. 1 del d.p.r. 445/'00, viene disciplinata nelle modalità e nei limiti di generazione e utilizzo alla V sezione del capo II del medesimo decreto.

Ai sensi della lettera n) del sopra citato art. 1, per firma digitale si intende "il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

La criptografia, su cui si basa anche il sistema di chiavi asimmetriche a coppia di cui sopra, è una metodologia di elaborazione di algoritmi atti a rendere non "leggibile" un qualunque documento (inteso nella più ampia accezione del termine) se non attraverso una "chiave". Quest'ultima è una

stringa, ossia una sequenza finita di caratteri che, interagendo con l'algoritmo alla base del metodo di computazione crittografico, consente di codificare e decodificare il documento.
Il metodo a chiave asimmetrica consta di una coppia di stringhe, differenti e combinate, per la codifica e la decodifica del documento, costruite in modo tale che, da un lato, un messaggio criptato con una delle due chiavi possa essere correttamente decifrato solo ed esclusivamente attraverso l'altra e, dall'altro, che pur conoscendo una chiave, da essa non si possa ricavare l'altra.
Il processo, al contrario del sistema a chiave simmetrica che prevede una sola stringa per la codificazione e la decodificazione, garantisce, attraverso la combinazione della coppia di chiavi asimmetriche, un più ampio margine di sicurezza, che deve comunque essere valutato in base alla probabilità di riuscire, in un tempo sufficientemente breve, a ricavare la stringa mancante; sotto l'aspetto computazionale, infatti, ottenere l'esatta sequenza di caratteri che compongono la stringa non è impossibile, ma solo estremamente arduo. La complessità di una ricerca metodica della chiave mancante, ossia il numero di operazioni elementari che si debbono compiere per ottenere il risultato, aumenta esponenzialmente all'aumentare della lunghezza (in *bit*) della stringa e determina, in relazione alla tecnologia (in continua evoluzione) di cui si dispone, il tempo medio necessario per "violare" il sistema. In altri termini, all'aumentare della lunghezza della chiave, aumenta esponenzialmente il numero delle operazioni necessarie per ottenerla e, di conseguenza, cresce proporzionalmente la sicurezza del sistema. In tal senso, l'allegato tecnico al d.p.r. 513/'97 (emanato con decreto del Presidente del Consiglio dei Ministri l'8 febbraio 1999), all'art. 4 specifica che le chiavi debbono avere una lunghezza minima di 1024 bit, mentre alla lettera f) dell'art. 22 del d.p.r. 445/'00 [art. 1, lett. h), d.p.r. 513/'97], è disposto che le chiavi abbiano una validità limitata nel tempo a tre anni, ritenendo che, sulla base delle tecnologie attualmente a disposizione e tenuto conto dell'evoluzione nel tempo delle stesse, un simile sistema è *probabilisticamente* inviolabile.

4. LA FIRMA DIGITALE NELLA PREVISIONE DEL D.P.R. 445/'00

L'impianto legislativo prevede che la coppia di chiavi sia composta da una chiave privata e da una pubblica; attraverso la chiave privata, conosciuta solo dal soggetto titolare, "si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la chiave pubblica" (Art. 22, lett. c), d.p.r. 445/'00); con la chiave pubblica "si verifica la firma digitale

apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi" (Art. 22, lett. d), d.p.r. 445/'00).

La chiave pubblica è rilasciata da un ente certificatore, che secondo la previsione del regolamento può essere sia pubblico che privato ed al quale è attribuito il compito, da un lato, di effettuare la certificazione, di rilasciare e pubblicare il certificato della chiave pubblica e di pubblicare ed aggiornare gli elenchi dei certificati sospesi e revocati (Art. 22, lett. i), d.p.r. 445/'00) e, dall'altro, di provvedere alla revoca od alla sospensione del certificato, di identificare con certezza la persona che fa richiesta della certificazione, di rilasciare e rendere pubblico il certificato e di specificare - su richiesta dell'istante e previo consenso del terzo interessato - la sussistenza dei poteri di rappresentanza, attenendosi alle misure minime di sicurezza per il trattamento dei dati personali di cui all'art. 15, II comma, della legge 675/'96 (Art. 28, II comma, d.p.r. 445/'00). Per certificazione si intende "il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave, ed il termine di scadenza del relativo certificato, in ogni caso non superiore ai tre anni" (Art. 22, lett. f), d.p.r. 445/'00).

La firma digitale, inoltre, come previsto al III comma dell'art. 23 del regolamento [art. 10, comma 3, d.p.r. 513/'97], "deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata" e, attraverso essa, debbono potersi rilevare, ai sensi del VII comma del medesimo articolo, "gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione" [art. 10, comma 7, d.p.r. 513/'97].

Nelle transazioni tra due (o più) parti, il sistema di chiavi asimmetriche consente tre differenti possibilità di combinazione cui conseguono tre diversi livelli di sicurezza dello scambio telematico.

La prima possibilità consiste nel cifrare il documento che si intende inviare al destinatario con la propria chiave privata; il destinatario potrà decifrarlo attraverso la chiave pubblica del mittente. Questo sistema, previsto esplicitamente nell'ambito delle definizioni di chiave pubblica e privata di cui alle lettere c) e d) dell'art. 22 del d.p.r. 445/'00 [art. 1, lett. e) e f), d.p.r. 513/'97], pur garantendo al destinatario la paternità del documento che riceve, non può considerarsi sicuro dal punto di vista della riservatezza in quanto chiunque ne entri in possesso può decodificarlo applicando la chiave pubblica del mittente.

La seconda eventualità consiste nell'inversione della precedente apposizione delle firme; in altri termini, il documento verrà cifrato dal mittente con la chiave pubblica del destinatario, il quale decifrerà lo stesso applicando la propria chiave privata. Questo metodo, quantunque atto a garantire la riservatezza del documento, non può essere equiparato alla previsione del regolamento riguardo la firma digitale, essendo non idoneo a garantire la corrispondenza tra il documento ed il suo presunto autore.

La terza modalità prevede l'utilizzo combinato tanto della chiave pubblica del destinatario, quanto della chiave privata del sottoscrittore; il mittente, dapprima codifica il documento con la propria chiave privata e, successivamente, con la chiave pubblica del destinatario, di modo che il destinatario, per riportare in chiaro il documento, dovrà apporgli la propria chiave privata e quindi la chiave pubblica del sottoscrittore mittente; il metodo può essere raffigurato da un sistema formato da due contenitori, uno esterno ed uno interno: quello esterno - contenente il contenitore interno che a sua volta contiene il documento - può essere aperto dal solo destinatario con l'apposizione della propria chiave privata e, una volta aperto, quello interno potrà essere aperto dal destinatario medesimo solamente "inserendo" la chiave pubblica del mittente. In tal modo si ottiene il duplice risultato, da un lato, di rendere la trasmissione riservata, in quanto il documento criptato - anche cadendo in mani sbagliate - non potrà essere decodificato se non con la chiave privata del legittimo destinatario e, dall'altro, di garantire al destinatario la certezza sulla paternità del documento ricevuto, in quanto solo con l'apposizione della chiave pubblica del destinatario si potrà decodificare il documento.

Da quanto sinora detto, quest'ultima metodologia di utilizzo della firma digitale "sembra" garantire una maggior sicurezza delle transazioni; sembra, in quanto, come precedentemente accennato, "violare" il sistema trovando la "stringa mancante" dell'algoritmo, quantunque *probabilisticamente* impossibile, considerata la lunghezza della stringa, non è completamente da escludere. Ciò in quanto, se è pur vero che i tempi medi di computazione sono talmente lunghi che si può ritenere *probabilisticamente* inviolabile la stringa, è altrettanto vero che, essendo la chiave una sia pur lunghissima sequenza di caratteri, essa è comunque una sequenza *finita*, il che implica un numero finito di possibilità di combinazione dei caratteri componenti una stringa anche a 1024 bit. Per cui, di fatto, anche se estremamente improbabile, la sequenza esatta potrebbe essere trovata casualmente anche al primo tentativo!

In un prossimo futuro la sicurezza delle transazioni telematiche subirà una svolta con la diffusione delle chiavi biometriche, ossia dei codici informatici che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente, come ad esempio l'impronte digitali o

la mappatura della retina, chiavi già previste alla lettera e) dell'art. 22 del d.p.r. 445/'00 [art. 1, lett. g), d.p.r. 513/'97], ma che per il momento non hanno una larga diffusione, dati i costi commerciali delle apparecchiature di verifica.

Un ulteriore aspetto riguarda la possibilità di apporre al documento informatico una validazione temporale. L'art. 4 del d.p.c.m. prevede, infatti, accanto alle chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti, altre due differenti tipologie di chiavi: le chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati ed alle loro liste di revoca o sospensione e le chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali. In tal senso, la norma di cui all'art. 58 del d.p.c.m., in attuazione della previsione della lettera g) dell'art. 22 del d.p.r. 445/'00 [art. 1, lett. i), d.p.r. 513/'97] , ove si specifica che la validazione temporale è il risultato della procedura informatica con cui si attribuiscono ad un documento informatico una data ed un orario opponibili ai terzi, disciplina la richiesta di validazione temporale, delegando al certificatore le procedure per l'inoltro della richiesta medesima; richiesta che deve contenere l'evidenza informatica alla quale le marche temporali debbono fare riferimento.

5. LA CERTIFICAZIONE DELLE CHIAVI E GLI ENTI CERTIFICATORI

Con il procedimento di certificazione e attraverso la pubblicazione della chiave pubblica, la firma digitale può essere legalmente utilizzata ai fini previsti dal regolamento.

I singoli certificatori, iscritti nell'elenco dei certificatori dell'AIPA hanno il compito di identificare con certezza la persona che fa richiesta della certificazione e di rilasciare e di rendere pubblico il certificato. Lo scopo della certificazione è infatti quello di rendere certo e conoscibile il rapporto biunivoco tra l'identità del richiedente e la propria firma digitale al fine di garantire i terzi che entreranno in rapporto con il soggetto. In tal senso, l'art. 28 del d.p.r. 445/'00 prevede che l'ente certificatore, su richiesta dell'interessato e con il consenso del terzo interessato, specifichi la sussistenza di poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite. Ulteriori compiti del certificatore riguardano il procedere tempestivamente alla revoca o alla sospensione del certificato a fronte della richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o

falsificazioni. Inoltre l'ente deve dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche.
Ai sensi dell'art. 27 del Testo unico 445/'00, in riferimento alla certificazione delle chiavi, l'attività di certificazione vengono effettuate da certificatori inclusi nell'elenco pubblico dei certificatori, consultabile in via telematica, predisposto, tenuto e aggiornato a cura dell'AIPA. Detti enti debbono avere la forma giuridica di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria e debbono essere in grado di garantire la qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.
I rappresentanti legali degli enti ed i soggetti preposti all'amministrazione debbono essere in possesso dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche.

6. EFFICACIA PROBATORIA

L'art. 10 del d.p.r. 445/'00 combina, senza modificarli nel contenuto, gli artt. 4 e 5 dell'abrogato d.p.r. 513/'97. Il I comma dell'art. 4, d.p.r. 513/'97, disponeva che "il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta"; il I comma dell'art. 5, d.p.r. 513/'97, prevedeva che "il documento informatico, sottoscritto con firma digitale ai sensi dell'art. 10, ha efficacia di scrittura privata ai sensi dell'art. 2702 del codice civile"; ai sensi del II comma, inoltre, "il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare".
Ai sensi dell'art. 10 del d.p.r. 445/'00, il documento informatico conforme alle disposizioni di cui all'art. 8 del d.p.r. 445/'00 [artt. 2 e 3, d.p.r. 513/'97] e sottoscritto con firma digitale [art. 22, d.p.r. 445/'00], oltre a soddisfare il requisito legale della forma scritta, ha efficacia di scrittura privata in virtù del richiamo, operato dal disposto di cui al III comma dello stesso, all'art. 2702 c.c., ove si prevede che la scrittura privata fa piena prova, fino a querela di falso, che le dichiarazioni in essa contenute provengono dal sottoscrittore, "se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta"; inoltre al medesimo documento è attribuita efficacia probatoria ai sensi dell'art. 2712 c.c.

In merito al riconoscimento (*rectius*: disconoscimento) della sottoscrizione si deve rilevare una sostanziale differenza tra la sottoscrizione tradizionale e la firma digitale.

A fronte del disconoscimento della sottoscrizione tradizionale previsto all'art. 214 c.p.c. la controparte che intende valersi della scrittura privata disconosciuta, può proporre istanza di verificazione; attraverso una perizia calligrafica si può, in vero, dimostrare l'autenticità della sottoscrizione autografa.

In base al disposto di cui all'art. 10 del d.p.r. 445/'00 [art. 5, comma 1, d.p.r. 513/'97], dato il rinvio all'art. 2702 c.c., è altresì possibile, da un lato, disconoscere la sottoscrizione digitale e, dall'altro, esperire istanza di verificazione. Ma la sottoscrizione digitale, come è stato precedentemente chiarito, essendo sostanzialmente un codice informatico non ha i requisiti della autografia, della leggibilità e della nominatività. Se attraverso un procedimento cripto-analitico si riesce a "decifrare" il codice della firma digitale, il codice ottenuto è *identico* all'originale, è l'originale.

Attraverso una perizia grafologica si riesce a stabilire se una firma tradizionale è stata apposta da un soggetto diverso dal presunto sottoscrittore, in quanto la forma e l'inclinazione dei segni, le eventuali interruzioni tra lettere, la pressione della penna sulla carta, ecc., sono unici e differiscono da soggetto a soggetto; anche a fronte di una falsificazione praticamente perfetta, quindi *apparentemente identica* alla firma originale del sottoscrittore, una perizia accurata riesce a rilevare differenze.

In caso di apposizione della firma digitale da parte di un soggetto che non ne è titolare, sia a seguito di "falsificazione" della firma digitale, sia a seguito di furto o cessione volontaria a terzi della firma digitale, non è dimostrabile il "falso", in quanto il codice (una serie di numeri e lettere) è esattamente lo stesso che avrebbe apposto il titolare della firma digitale. Per intendersi, è come se si sottoscrivesse un documento cartaceo apponendo il proprio nome e cognome con una macchina da scrivere: si potrebbe stabilire il tipo di macchina, il tipo di inchiostro usato, ma non sarebbe dimostrabile che quella "firma" è stata apposta dal titolare della medesima, piuttosto che da altra persona.

Riguardo i casi sopra descritti di apposizione della firma digitale da parte di un soggetto non titolare della medesima, si riflette in dottrina sulla riconducibilità di essi all'istituto della rappresentanza. In riferimento all'istituto della rappresentanza, si deve operare una distinzione tra la firma digitale "falsa", ossia apposta da un soggetto diverso dal titolare senza l'autorizzazione del medesimo e la firma apposta da un soggetto autorizzato dal titolare ma non indicato all'ente certificatore, riflettendo per il primo caso sull'ipotesi di *falsus procurator* ovvero sulla rappresentanza apparente, mentre per il secondo sulla spendita tacita del nome del rappresentato.

In riferimento all'onere probatorio della autenticità della firma a carico di chi ne invoca l'efficacia, esso è quasi una mera formalità, in quanto sarà sufficiente provare la corrispondenza tra chiave pubblica e privata per avere la certezza che quella firma digitale corrisponde a quel determinato soggetto; ciò però non significa necessariamente che sia stato detto soggetto ad apporla, ma ciò viene presunto. Al contrario, per disconoscere la propria firma digitale sarà necessario dar prova dell'esclusione di responsabilità della sottoscrizione, cosa affatto agevole; di fatto la presunzione di appartenenza al soggetto titolare della firma digitale apposta è necessaria al funzionamento dell'intero sistema.

L'impianto della legge prevede, a carico del titolare della firma digitale, l'obbligo di mantenere assolutamente segreta la chiave privata e la possibilità di richiedere la revoca all'ente certificatore, il quale ente ha l'obbligo, ai sensi dell'art. 28 del regolamento [art. 9, d.p.r. 513/'97], di procedere tempestivamente alla revoca od alla sospensione del certificato e di dare immediata pubblicazione della revoca o della sospensione della coppia di chiavi asimmetriche; ciò consente il disconoscimento delle firme apposte dopo la richiesta di revoca, in quanto la presunzione di appartenenza non opera se la corrispondente chiave pubblica è scaduta o revocata. Ai sensi dell'art. 23 del regolamento [art. 10, d.p.r. 513/'97], infatti, "l'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate" (art. 23, punto 5, d.p.r. 445/'00). In tal senso, può avere ulteriore rilevanza l'apposizione della validazione temporale al documento informatico sottoscritto con firma digitale, come previsto alla lettera g) dell'art. 22 del d.p.r. 445/'00 [art. 1, lett. i), d.p.r. 513/'97], per una maggiore certezza giuridica nella misura della sua opponibilità ai terzi.

7. LA FIRMA DIGITALE AUTENTICATA E L'ATTO PUBBLICO

In base al disposto di cui all'art. 24 del d.p.r. 445/'00 [art. 16, d.p.r. 513/'97], rubricato sotto la dizione "firma digitale autenticata", la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato, si ha per riconosciuta ai sensi dell'art. 2703 c.c.; il secondo comma stabilisce che il pubblico ufficiale autentica la firma digitale attestando, previo accertamento dell'identità personale del titolare della firma, della validità della chiave utilizzata e del fatto che il

documento sottoscritto corrisponde alla volontà della parte e che non è in contrasto con l'ordinamento giuridico (come previsto all'art. 28, I comma, n. 1, della legge notarile n.89 del 16 febbraio 1913), che la firma digitale è stata apposta in sua presenza dal titolare. In altri termini, compito del pubblico ufficiale sarà accertare la corrispondenza tra sottoscrittore e chiave pubblica attraverso la verifica del certificato, controllare che la chiave pubblica non sia scaduta, revocata o sospesa ed accertare la corrispondenza della chiave pubblica con la chiave privata; in tal senso, dato che ogni soggetto può essere titolare di più firme digitali, il sottoscrittore dovrà criptare e decriptare il documento innanzi al notaio per le verifiche e, successivamente, cifrarlo definitivamente; ciò fatto, il notaio autenticherà il documento apponendo la propria firma digitale.

Inoltre, ai sensi del IV comma dell'art. 24 del d.p.r., per il caso in cui al documento informatico autenticato debba essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'art. 20, comma 3, del medesimo regolamento [art. 6, d.p.r. 513/'97], ove è previsto che le copie su supporto informatico di documenti (formati in origine su supporto non informatico) sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico in conformità con le modalità indicate dal regolamento. In proposito ci si interroga sull'obbligo per il notaio di conservare il documento cartaceo originale, dato che la legge nulla dice in merito, anche se sembra doversi ritenere che l'obbligo permanga come giustamente argomentato in dottrina.

Una ulteriore questione riguarda l'ammissibilità del c.d. atto pubblico informatico, ossia il documento informatico redatto con le formalità prescritte per l'atto pubblico *ex* art. 2699 c.c., dato che il d.p.r. 445/'00, (come del resto anche l'abrogato d.p.r. 513/'97) non ne fa menzione. In riferimento a ciò, si segnalano due contrapposte posizioni dottrinali, l'una che, sulla base della mancata previsione normativa, nega assolutamente la possibilità di stipulare un atto pubblico informatico; l'altra che, argomentando al contrario, ammette l'eventualità proprio per l'assenza di un esplicito divieto normativo. In tal senso, si deve altresì sottolineare l'astratta compatibilità delle formalità prescritte per l'atto pubblico con il documento informatico, sebbene qualche perplessità può essere sollevata sulla concreta necessità di un tale atto, dato che esso non può essere stipulato telematicamente, dunque a distanza, essendo prescritta la presenza di tutte le parti contrattuali per la lettura dell'atto stesso da parte del notaio o del pubblico ufficiale autorizzato; anche se si potrebbe astrattamente prevedere il caso di presenza, non fisica, delle parti tramite videoconferenza, purché, ad esempio, ogni parte partecipi all'atto pubblico per videoconferenza da una sede notarile (secondaria) di fronte ad un notaio

che, nel qual caso, non avrebbe funzione rogante ma di mero garante della identità del parte a lui di fronte e del corretto svolgimento della procedura. Riflettendo sulla recente iniziativa del Consiglio Nazionale del Notariato volta alla realizzazione di una rete interna di collegamento telematico degli studi notarili (che permetterà l'interconnessione anche con la Pubblica Amministrazione), questa eventualità potrebbe essere, in un futuro prossimo, percorribile.

Stampato presso la sede della Fondazione – maggio 2001