INFORMATICA E DIRITTO: IL DOCUMENTO INFORMATICO E LA FIRMA ELETTRONICA

Alessandro MATURO
Laureato in Giurisprudenza nell'Università di Parma
Collaboratore volontario nell'Università di Chieti

SOMMARIO: In questo lavoro si analizzano i concetti di documento e firma da un punto di vista giuridico. Si mostra come anche file su disco rigido o floppy disk, opportunamente trattati, soddisfano ai requisiti richiesti ad un documento. Infine si mostra come il problema della firma di un documento e della sua autenticazione possono essere ben risolti anche per i documenti informatici con garanzia di autenticità addirittura superiore rispetto ai documenti cartacei.

1. DOCUMENTO E FIRMA

Il concetto di documento è la sintesi di due elementi essenziali:

a) dal punto di vista strutturale, il documento è il contenente, la cosa, il supporto in cui l'idea viene rappresentata e che è idoneo a conservarla a distanza di tempo; tale supporto può essere di varia natura: la tradizionale carta su tutti, ma anche altri materiali quali la pietra, il legno, un nastro magnetico, un *floppy disk*, un CD-ROM, etc.;

b) dal punto di vista funzionale, il documento è il contenuto, l'idea rappresentata nella cosa, idea che, all'atto della rappresentazione, modifica materialmente la cosa: sarà l'inchiostro sulla carta, la pietra scolpita, il legno intarsiato, il disco ottico inciso, etc..

Perché si parli correttamente di documento, dunque, sono necessari entrambi gli elementi: se c'è la materia senza contenuto, non c'è un documento, ma una cosa; se c'è il contenuto senza la materia, non c'è un documento, ma un'idea. La mente umana è portata a materializzare i concetti astratti, a trasformarli nelle cose che vediamo e tocchiamo; così, spesso si dice: "il documento è il pezzo di carta"; non è vero: un pezzo di carta è un pezzo di carta, non un documento; diventa un documento solo se viene a rappresentare un fatto (ad esempio, un contratto di vendita).

Il documento, dunque, è sintesi di contenente e contenuto. Il contenente è un supporto materiale, cioè, si è visto, una cosa idonea a conservare un contenuto. La materialità del supporto svolge, nel documento, una precisa funzione: quella di garantire l'originale consistenza e contenuto del documento, in una parola, la sua integrità. Ma affinché questa funzione sia svolta pienamente, occorre che il supporto sia

indelebile, cioè non consenta cancellazioni di quanto in esso è stato scritto o, quanto meno, mantenga traccia delle eventuali alterazioni, in modo che qualsiasi modifica sia riconoscibile.

Tale funzione è svolta dalla carta: non si può cancellare l'inchiostro senza modificare fisicamente il materiale cartaceo.

Si è visto che, in generale, un documento rappresenta un fatto. Una particolare categoria di fatti c'interessa più da vicino: quella degli atti, vale a dire i fatti compiuti dall'uomo per sua iniziativa volontaria. Orbene, un atto può essere rappresentato in un documento; ma da chi proviene quest'atto? A chi è imputabile? Il modo tradizionalmente usato per verificare la provenienza soggettiva (c.d. imputabilità) di un atto contenuto in uno scritto è la sottoscrizione, cioè l'apposizione autografa (-scrizione) del proprio nome in calce (sotto-) ad un documento di cui si vuole assumere la paternità.

La sottoscrizione svolge in modo esemplare tale funzione, dato che essa è personale, unica per ogni individuo: i grafologi c'insegnano che ciascuno di noi ha un modo di scrivere diverso da tutti gli altri, perché la grafia riflette la personalità, l'io interiore; non è possibile, dunque, riprodurre perfettamente la scrittura (e quindi la sottoscrizione) di una persona: un grafologo (e spesso anche una persona senza particolari competenze) saprà sempre cogliere la differenza.

La sottoscrizione ha, oltre a quella appena accennata (la personalità), altre caratteristiche, tutte coessenziali al concetto:

a) immodificabilità e non riutilizzabilità. La sottoscrizione non può essere alterata né prelevata e riutilizzata in altro documento, in quanto legata indissolubilmente al supporto. E qui sta l'anello di congiunzione tra supporto e garanzia di provenienza soggettiva del documento: l'indelebilità del supporto garantisce, oltre all'integrità del documento, l'immodificabilità e la non riutilizzabilità della sottoscrizione e, di conseguenza, l'imputabilità del documento;
b) autografia.)"La sottoscrizione deve essere apposta di proprio pugno o, come suol dirsi, a mano libera";
c) nominatività. La sottoscrizione deve contenere il prenome e il cognome del sottoscrivente;
d) leggibilità. "La sottoscrizione deve essere apposta a tutte lettere, in maniera chiara, sempre facilmente leggibile".

Il carattere della leggibilità, insieme con quello dell'autografia e della nominatività, fonda un altro carattere della sottoscrizione: la riconoscibilità, che permette di identificarne l'autore; questo è un carattere essenziale della sottoscrizione, in quanto le permette di svolgere la sua funzione.

La sottoscrizione svolge essenzialmente la funzione di creare una relazione tra il soggetto che sottoscrive e il documento; relazione che chiamiamo di provenienza soggettiva (o imputabilità). Ma cosa significa che un documento proviene da un soggetto (o, che è lo stesso, è imputabile ad un soggetto)? La risposta a questa domanda ci porta a specificare la generica funzione della sottoscrizione in:

a) funzione indicativa: la sottoscrizione indica, cioè individua, l'autore del documento;
b) funzione dichiarativa: con la sottoscrizione del documento, l'autore dichiara di assumerne la paternità.

La funzione dichiarativa della sottoscrizione è strettamente legata ad una delle funzioni essenziali della forma vincolata: assicurare la ponderatezza delle decisioni: nel compiere un atto a forma vincolata (es. atto pubblico), un soggetto deve 'superare delle difficoltà' (es. andare dal notaio, sottoscrivere alla presenza di costui, etc.) che richiamano la sua attenzione sull'importanza dell'atto di cui si sta assumendo la paternità;

c) funzione probatoria: il documento sottoscritto fa prova della provenienza del documento stesso dal soggetto che ha apposto la sottoscrizione (sotto entrambi i profili *sub* a) e *sub* b)).

Anche qui troviamo un notevole punto di contatto tra funzione della sottoscrizione e funzione della forma vincolata: entrambe rispondono ad un'esigenza di documentazione, vale a dire di certezza e conoscibilità (pubblicità) degli atti.

Le tre funzioni ora descritte non sono tre realtà diverse: sono tre profili di un'unica realtà, vale a dire della provenienza esclusiva del documento dal suo autore. È sempre la stessa realtà, ma guardata da punti di vista diversi: dal punto di vista dei soggetti 'altri' rispetto all'autore, che individuano l'autore stesso dalla sottoscrizione (funzione indicativa); dal punto di vista dell'autore del documento, che dichiara di assumerne la paternità proprio con la sottoscrizione (funzione dichiarativa); dal punto di vista del giudice di un'eventuale controversia, che assumerà il documento sottoscritto come prova della sua provenienza dal sottoscrittore (funzione probatoria).

La sottoscrizione non è, però, l'unico modo di imputare un documento scritto ad un soggetto: è sicuramente il modo più diffuso, ma è solo uno dei modi, non certo l'unico. L'osservazione va approfondita sotto due profili: in diritto e in fatto.

Da un punto di vista giuridico in senso stretto, cioè *de iure condito*, vi sono norme legislative e orientamenti giurisprudenziali che evidenziano altri modi d'imputazione che si considerano giuridicamente rilevanti.

E così l'art. 27051 c.c. attribuisce l'efficacia probatoria delle scritture private al telegramma, "se l'originale consegnato all'ufficio di partenza è sottoscritto dal mittente, ovvero è stato consegnato o fatto consegnare dal mittente medesimo senza sottoscriverlo". La provenienza del telegramma, che ovviamente non può essere sottoscritto, è garantita dunque o dalla sottoscrizione dell'originale consegnato all'ufficio abilitato a spedire il telegramma, o dal mero fatto della consegna da parte del mittente (o di un suo incaricato).

La giurisprudenza, dal canto suo, (e passiamo così ad un secondo caso), considera la produzione in giudizio di un atto (processuale) come equivalente alla sottoscrizione dell'atto stesso.

Infine, la pratica dei titoli di credito (nella specie i titoli di massa, cioè azioni e obbligazioni) ha comportato la diffusione della sottoscrizione apposta a stampa o con altri mezzi meccanici, comunque non autografa.

Da un punto di vista fattuale, giuridico solo in prospettiva futura, *de iure condendo*, accade che "i soggetti dell'economia moderna non comunicano più con lettere firmate dal mittente, ma attraverso segni trasmessi da apparati meccanici (telegramma su originali scritti, telegramma dettato per telefono, tel*ex*, telecopier, etc.). Il risultato dell'attività espressiva è sempre in un testo scritto, ma sprovvisto di firma autografa. Il requisito della sottoscrizione, storicamente legato al contratto tra persone presenti e all'uso sociale delle lettere missive, si scopre ormai incompatibile con le moderne tecniche di fissazione e trasmissione della parola. I messaggi scritti vogliono liberarsi dal vincolo della firma, e perciò sollecitano nuovi metodi di imputazione, mai criteri di riferimento alla persona del dichiarante. Metodi e criteri non più legati alla firma autografa, ma all'uso esclusivo dell'apparato tecnico: codesta esclusività terrà il luogo della personalità della sottoscrizione."

Questa situazione viene chiamata "crisi della sottoscrizione".

Tale "crisi" è destinata a peggiorare con l'avvento dell'era informatica: il documento elettronico, pur essendo considerato documento scritto, non può essere sottoscritto in un modo tradizionale.

Bisognerà, dunque, individuare uno (o anche più d'uno) strumento informatico equivalente alla sottoscrizione, cioè diverso da essa, ma idoneo a svolgerne la funzione. Quest'indagine sarà oggetto del par. 3.

Ma andiamo con ordine ed esaminiamo, prima, la nozione di documento elettronico.

2. DOCUMENTO INFORMATICO

Il documento elettronico (o informatico) è, dunque, un documento scritto su un supporto informatico. La 'scrittura' consiste essenzialmente in una sequenza di *bit* memorizzati nel supporto: essi non possono essere letti direttamente dall'uomo, ma devono prima essere 'tradotti' dal *computer* in forma comprensibile all'uomo e in ciò risiede una grande differenza, soprattutto psicologica, rispetto al tradizionale documento cartaceo. Questa definizione, da tempo introdotta in dottrina, è oggi nel diritto positivo: il d.P.R. sul documento elettronico definisce il "documento informatico" come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1 lett. a)) e precisa che esso, "munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta" (art. 41). È, in sostanza, la definizione classica di 'documento', con l'aggiunta dell'aggettivo 'informatico'; ed è, al di là di mere questioni di parole, la stessa definizione da noi ricostruita subito *retro*.

L'appena citato d.P.R. 10 novembre 1997, n. 513 ("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della l. 15 marzo 1997, n. 59") è finalmente intervenuto a disciplinare il documento informatico, accogliendo le posizioni della più autorevole dottrina specialistica.

Si tratta di una disciplina generale, redatta per principi, una specie di 'diritto comune informatico', che rinvia ad altre fonti subordinate (provvedimenti di organi governativi o di singole Pubbliche Amministrazioni, sempre in collaborazione con l'AIPA) la disciplina degli aspetti tecnici della materia. Il che è ben comprensibile: la rapida evoluzione dell'informatica rende ben presto obsolete norme appena'confezionate', sicché solo un organo con competenze tecniche *ad hoc* (l'AIPA), non certo un organo politico quale il Parlamento, è in grado di disciplinare adeguatamente il fenomeno, seguendo tutti gli sviluppi della tecnologia. La stessa definizione di documento informatico nasce come definizione 'evolutiva': esso, per l'art. 4 è documento scritto se "munito dei requisiti previsti dal presente regolamento" e, cioè, se conforme alle "regole tecniche" dettate *ex* art. 31 e rinnovate a scadenze almeno biennali *ex* art. 32.

Il documento informatico, se formato nel rispetto delle disposizioni del regolamento sul documento elettronico, è valido e rilevante a tutti gli effetti di legge (art. 02).

Ma in che cosa consiste questa "rilevanza"? Qual è l'efficacia probatoria del documento informatico?

Il regolamento delinea un sistema così composto:

a) documento informatico senza firma digitale: ha l'efficacia probatoria propria delle riproduzioni meccaniche *ex* art. 2712 c.c.: fanno "piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti e alle cose medesime" (art. 5 regol. docum. inform., che rinvia all'art. 2712 c.c.);
b) documento informatico 'sottoscritto' con firma digitale: ha l'efficacia probatoria della scrittura privata *ex*) art. 2702 c.c. (art. 5 regol. docum. inform., che rinvia all'art. 2702 c.c.). Tale norma è logico corollario del principio generale dell'equivalenza tra sottoscrizione tradizionale e firma digitale, stabilito dall'art. 10;
c) documento informatico 'sottoscritto' con firma digitale autenticata: ha l'efficacia probatoria della scrittura privata con sottoscrizione autenticata *ex* art. 2703 c.c. (art. 161 regol. docum. inform.). L'autenticazione consiste nell'attestazione, da parte di un notaio o di un pubblico ufficiale autorizzato, che "la firma digitale è stata apposta in sua presenza dal titolare", previo accertamento di:
   I) identità personale del sottoscrittore;
   II) validità della chiave utilizzata;
   III) rispondenza del documento alla volontà della parte;
   IV) conformità del documento con l'ordinamento giuridico, "ai sensi dell'art. 28, n. 1, l. 16 febbraio 1913, n. 89 [legge notarile]" (art. 162 regol. docum. inform.).

Il notaio o il pubblico ufficiale effettua tale autenticazione, com'è naturale, apponendo al documento informatico sottoscritto dal soggetto la propria firma digitale. L'apposizione della firma digitale da parte del notaio o del pubblico ufficiale integra e sostituisce, ad ogni fine di legge, l'apposizione di sigilli, punzoni, contrassegni e marchi comunque previsti (art. 163 regol. docum. inform.).

Date queste premesse, il documento informatico con firma digitale autenticata si presta ad applicazioni straordinarie: non solo tutti gli atti giuridici ammessi nel nostro ordinamento (salvo quelli che richiedono la forma dell'atto pubblico) potranno perfezionarsi, in originale, in forma esclusivamente elettronica; ma i documenti elettronici che ne risulteranno potranno essere direttamente immessi nei pubblici registri, quali ad es. i registri immobiliari e il registro delle imprese, anche mediante trasmissione in via telematica.

Ma non basta: si è visto che documento informatico è la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1 lett. a)); tale rappresentazione può avere (e normalmente ha) ad oggetto un testo scritto a parole; ma può avere ad oggetto anche immagini, filmati, suoni, etc. e qualunque altra realtà digitalizzabile. Orbene, vere queste premesse, potremo avere nel nostro ordinamento scritture private non testuali, che documentano atti svolti in altra forma, ad esempio orali; così, ad esempio, accanto al testamento olografo, potrebbe assumere valore il testamento nuncupativo.

Abbiamo visto che, nel sistema del regol. docum. elettr., il documento elettronico, dal punto di vista giuridico, può avere valore, a seconda dei casi, di riproduzione meccanica o di scrittura privata. Ma può esistere un documento elettronico che abbia valore di)atto pubblico? Da un punto di vista tecnico-informatico, non ci sarebbero problemi. Ma da un punto di vista giuridico, dobbiamo escludere che possano essere formati, da notai o altri pubblici ufficiali equiparati, atti pubblici elettronici: le caratteristiche tecnico-giuridiche dell'atto pubblico (complessità della legge notarile; in particolare, sarebbe sempre necessaria la contestuale presenza delle parti davanti al notaio) lo sconsigliano: per questa ragione il regolamento sul documento elettronico non ha previsto tale possibilità.

Ma questo discorso vale per gli atti pubblici formati in originale, non per le copie in forma elettronica di atti pubblici in originale cartaceo: "le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3" (art. 63).

Non è ammissibile, dunque, un atto pubblico elettronico in originale, ma è ammissibile un atto pubblico elettronico copia di un originale cartaceo e che ha, come l'originale, valore di atto pubblico. Naturalmente tale copia dovrà essere rilasciata da un pubblico ufficiale che la firmerà elettronicamente, attribuendole così pubblica

fede. Ma, una volta formata tale copia, si potranno ricavare da essa duplicati con piena efficacia probatoria, senza bisogno dell'intervento del notaio-.

I documenti elettronici con firma digitale autenticata e le copie elettroniche di atti pubblici cartacei, valendo rispettivamente come scritture private autenticate e come atti pubblici, hanno senz'altro data (e ora) certa opponibile ai terzi: vale il momento in cui il notaio appone la firma digitale.

Tutti gli altri documenti, per avere "una data e un orario opponibili ai terzi", devono assoggettarsi ad una particolare procedura informatica: il documento è affidato ad un certificatore (art. 58 d.P.C.M. reg. tecn.) che vi appone data e ora e sigilla il tutto con la sua firma digitale, sortendo un risultato analogo a quello della registrazione degli atti cartacei, vale a dire)l'opponibilità a terzi di data e ora; tale risultato è chiamato "validazione temporale" (art. 1 lett. i)).

A norma degli artt. 1 lett. f) e 52 d.P.C.M. reg. tecn., la validazione temporale, cioè l'apposizione di data e ora certe opponibili ai terzi, è operata mediante una marca temporale, una sorta di timbro digitale che attesta data e ora e che contiene una serie di altre informazioni (analiticamente elencate dall'art. 53; tra di esse, in particolare, l'identificazione dell'emittente la marca): il tutto sottoscritto digitalmente.

La marca temporale (cioè il *corpus* formato dai tre ordini di elementi ora descritti: ora e data - altre informazioni - sottoscrizione) è una sorta di firma digitale complessa: alla funzione della firma digitale (garantire provenienza e integrità del documento informatico) aggiunge una funzione ulteriore: la data e ora certe opponibili ai terzi (in tal modo integrando l'art. 2704 c.c.).

L'analogia con la firma digitale non è puramente funzionale, ma è anche strutturale: la marca temporale, infatti, come la firma, è generata da una coppia di chiavi; si tratta però di chiavi speciali, diverse dalle normali chiavi di sottoscrizione che permettono di generare la firma digitale: sono le chiavi di marcatura temporale (art. 44 lett. c).

L'art. 6 regol. docum. elettr. disciplina le copie di atti e documenti. Tre sono le ipotesi da considerare:

a) copie elettroniche di documenti elettronici: se spedite o rilasciate "da depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli artt. 2214 e 2215 c.c. [=fanno fede come l'originale copiato], se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente regolamento" (art. 62); pertanto, potremo avere:
   I) copie di documenti elettronici non firmati: valgono come riproduzioni meccaniche *ex* art. 2712 c.c.;
   II) copie di documenti elettronici firmati: valgono come scritture private *ex* art. 2702 c.c.;
   III) copie di documenti elettronici con firma autenticata: valgono come scritture private autenticate *ex* art. 2703 c.c.;

IV) copie di documenti elettronici copie di atti pubblici cartacei: valgono come atti pubblici *ex* art. 2700 c.c.;

b) copie elettroniche di documenti cartacei (caso già esaminato al punto 4): "sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratti se la loro conformità all'originale è autenticata da notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e osservata con la modalità indicata dal decreto di cui al comma 1 dell'art. 3" (art. 63);

c) copie cartacee di documenti elettronici: l'ipotesi non è espressamente disciplinata dal regolamento; si ritiene applicabile analogicamente l'art. 2719 c.c., che si riferisce alle "copie fotografiche di scritture"; pertanto le copie cartacee in questione hanno la stessa efficacia di documenti elettronici "se la loro conformità con l'originale è attestata da pubblico ufficiale competente ovvero non è espressamente disconosciuta".

Uno dei problemi fondamentali, oltre a quello di garantire l'integrità e provenienza del documento informatico, in un sistema di commercio e di amministrazione telematici è il problema del c.d. non ripudio del documento da parte del destinatario: come si fa a dimostrare che un documento inviato in via telematica è giunto al destinatario e, quindi, ad evitare che questi lo ripudi? Il destinatario potrebbe rilasciare telematicamente una ricevuta, ma il problema si pone proprio nei casi in cui egli non abbia alcun interesse a farlo.

L'art. 121 risolve il problema, stabilendo che il "documento informatico trasmesso via telematica s'intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato": si tratta, dunque, di una presunzione (relativa) di ricezione del documento inviato: spetta al mittente l'onere di provare l'invio del documento all'indirizzo elettronico dichiarato dal destinatario; spetta a quest'ultimo l'onere di provare di non aver ricevuto alcun documento: si tratta, in sostanza, di provare un caso di malfunzionamento della rete telematica, dei servizi ad essa inerenti o delle organizzazioni che li gestiscono (ad es. i c.d. *Internet Providers*).

Inoltre, se tale trasmissione avviene "con modalità che assicurano l'avvenuta consegna" del documento, essa "equivale alla notificazione per mezzo della posta", nei casi in cui essa è prevista dalla legge (art. 123).

La data e l'ora della formazione, trasmissione o ricezione del documento sono opponibili ai terzi, se il documento è redatto secondo le disposizioni del regolamento e le regole tecniche *ex* art. 3 (art. 122).

3. LA FIRMA ELETTRONICA

1. Si è visto al par. 1 che, nei tradizionali documenti cartacei, la sottoscrizione e la natura del supporto assicurano la provenienza e l'integrità del documento; si è anche parlato della "crisi della sottoscrizione" nella moderna società tecnologica.

Inoltre, al par. 2, si è visto come il supporto del documento possa essere diverso dalla tradizionale carta ed essere, in particolare, un supporto informatico.

Orbene, per il documento informatico la tradizionale sottoscrizione è del tutto inidonea ad assicurare la provenienza soggettiva e l'integrità del documento stesso.

Bisogna, dunque, trovare uno strumento tecnologico idoneo a svolgere la funzione propria della tradizionale sottoscrizione (nel suo triplice aspetto), pur non avendone i requisiti. A tale strumento, non definito nei suoi caratteri strutturali, ma individuato solo dal punto di vista funzionale, si dà il nome di "firma elettronica".

Il primo strumento cui si pensa è anche il più simile alla sottoscrizione tradizionale. Si tratta della 'sotto-scrizione elettronica', vale a dire una sottoscrizione autografa apposta con una speciale penna su una lavagnetta magnetica o elettronica in grado di leggerla e trasferirla nella memoria del *computer*, traducendola in *bit*.

È un espediente ingegnoso, che ripete tutti i caratteri tipici della tradizionale)sottoscrizione ed offre ottime garanzie di individuazione dell'autore (tramite l'analisi grafologica e dei parametri biodinamici della firma).

Esso, però, presenta un grave difetto: una volta memorizzata, può essere riutilizzata all'infinito per sottoscrivere documenti, spianando la strada ad usi abusivi d'ogni tipo. Ciò accade perché tale firma, una volta che si trova nella memoria del *computer*, è un dato statico, sempre uguale, che non si modifica a seconda dei documenti ai quali si riferisce.

Altro strumento al quale si può ricorrere per sostituire la tradizionale sottoscrizione è la c.d. firma biometrica, che si fonda sulla verifica dell'identità personale basata su specifiche caratteristiche fisiche dell'uomo: impronte digitali, vasi sanguigni della retina, timbro della voce, etc..

Questo strumento offre una sicurezza assoluta circa l'individuazione del soggetto a cui i caratteri fisici 'misurati' si riferiscono: ogni uomo ha caratteri suoi propri diversi da quelli di qualunque altro uomo.

Ciononostante, anche la firma biometrica non è idonea a sostituire la tradizionale sottoscrizione; e ciò, fondamentalmente, per due ragioni:

a) la firma biometrica è facilmente alterabile, dato che il supporto non è indelebile. Ma questo problema può essere superato utilizzando le memorie WORM (*Write Once Read Many*), memorie cioè di sola lettura, non riscrivibili (si Scrive Una Volta, si Legge Molte);
b) la firma biometrica, una volta fissata su un qualsiasi supporto informatico, è facilmente riutilizzabile: può essere copiata dal supporto e abusivamente usata per altri documenti; il che avviene, come già visto anche per la 'sottoscrizione elettronica', perché si tratta di una firma sempre uguale, non dipendente dal contenuto del documento 'sottoscritto'.

L'unico strumento finora ritenuto idoneo a sostituire la tradizionale sottoscrizione è la firma digitale. Essa è a) un insieme di caratteri alfanumerici, b) risultato di un algoritmo che elabora il contenuto di un documento, svolto sulla base di una c)

chiave crittografica. L'art. 1 lett. b) regol. docum. elettr. la definisce come "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"; laddove la procedura di "validazione" è una procedura informatica e crittografica "in grado di generare ed apporre la firma digitale o di verificarne la validità" (art. 1 lett. c)).

La firma digitale non ha assolutamente nulla a che fare con la tradizionale sottoscrizione: ne svolge la funzione, ma strutturalmente, è qualcosa di completamente diverso. Il che risulta evidente esaminando i singoli punti della definizione data.

(a) Il modo in cui la firma digitale si manifesta all'esterno, a chi la legge sul video di un *computer*, è un insieme di caratteri alfanumerici, cioè di lettere, numeri, simboli, etc.. Un esempio di firma digitale è:

——BEGIN PGP SIGNATURE——
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>

iQA/AwUBNiZQO9Qp7fuKGownEQJ1rgCbBpQ/+dZhascdx/Q3E3h/KhSdAR4AniAx
cyI6Kf/Cgon6yjeOGAoLHj+E
=Wbjo
——END PGP SIGNATURE——

Tale firma può trovarsi (e normalmente si trova) in calce al documento *de quo*; ma può anche trovarsi in separato documento informatico: questo è il senso dell'art. 101 regol. docum. elettr.: "a ciascun documento informatico [...] può essere apposta, o associata con separata evidenza informatica, una firma digitale".

(b) Ma quest'accozzaglia (apparente) di caratteri è solo il risultato esterno di complesse operazioni matematiche svolte dal *computer* seguendo la procedura descritta da un algoritmo crittografico.

Tale algoritmo è un insieme di istruzioni in sequenza, contenute in programma (es. PGP). Seguendo tali istruzioni, il *computer* svolge una procedura (c.d. validazione) che può essere così schematicamente descritta:

I] prende in considerazione il documento da firmare e la chiave crittografica (che nel sistema a chiavi asimmetriche è la chiave privata) da applicare al documento stesso;

II] svolge sul documento, sulla base della chiave crittografica, operazioni matematiche complesse: vale a dire, 'crittografa' (o 'cifra') il documento;

III] genera la firma digitale, come risultato delle operazioni matematiche svolte sul documento.

Come ben si vede, la fase I è preliminare: in essa il *computer* acquisisce i dati variabili concreti per poter svolgere le successive fasi della procedura; le due variabili della firma digitale sono, dunque, il documento e la chiave crittografica: se cambia una di queste, la firma sarà diversa; se entrambe restano uguali, la firma sarà uguale. La fase III, invece, è conclusiva: giunto a questo punto, il *computer* 'riversa' il risultato della procedura svolta, generando e visualizzando la firma digitale. Il cuore della procedura algoritmica, dunque, sta nella fase II, vale a dire nelle "complesse operazioni matematiche") svolte dal *computer*. Di che operazioni si tratta? Per rispondere a questa domanda si deve entrare nel campo (impervio per il giurista) degli studi matematici applicati alla crittografia.

Abbiamo parlato di "complesse operazioni matematiche" perché esse sono necessariamente tali nell'era del *computer*. In realtà, il concetto-chiave della crittografia è molto semplice e comprensibile a chiunque; lo si può cogliere appieno partendo dal metodo crittografico più facile e intuitivo, quello delle "lettere addizionate" (*additive ciphers*): ad ogni lettera di ciascuna delle parole che compongono un testo, viene sostituita un'altra lettera, di un numero x di posizioni avanti nell'ordine alfabetico; così, se x=3, la 'a' diventa 'd', la 'b' 'e', la parola 'atto' diventa 'dzzr', e così via. L'insieme di istruzioni che ordinano al *computer* tali sostituzioni è l'algoritmo. La x, che nell'esempio concreto è il numero 3, è la chiave crittografica: essa viene inserita dal *computer* nell'algoritmo per cifrare il testo. Il testo così cifrato è detto *ciphertext* (in contrapposizione a *plaintext*, il 'testo in chiaro'); nell'esempio fatto il *ciphertext* coincide con la firma digitale: ma non sempre è così; anzi, avere una firma digitale lunga come il testo è un inconveniente non da poco: occupa memoria del *computer*, rallenta le operazioni e anche graficamente, a colpo d'occhio, non sembra una firma. Si aggiunga che l'algoritmo appena descritto non è affatto sicuro, a causa della sua semplicità.

Per queste ragioni, gli algoritmi usati nella pratica sono ben più complicati. In particolare, per evitare che la firma digitale abbia la stessa lunghezza del testo firmato, sono stati ideati particolari algoritmi capaci di 'compattare' la firma alle dimensioni volute. Essi svolgono, in sintesi, le seguenti operazioni: dividono il testo in tanti blocchi di lunghezza n prefissata; cifrano il primo blocco; aggiungono il primo blocco così cifrato al secondo, in modo che ne risulti un blocco unico, sempre di lunghezza n (fanno ciò eseguendo particolari calcoli matematici; ad es. sommando le lettere corrispondenti dei due testi; così, se le prime tre lettere del primo blocco cifrato sono 'ame', e le prime tre lettere del secondo blocco 'nbi', la loro somma sarà 'ame' + 'nbi' = '(a+n)(m+b)(e+i) = 'oop'; 'oop' saranno le prime tre lettere del secondo blocco (a cui è stato aggiunto il primo già cifrato) cifrato); questo secondo blocco cifrato viene sommato al terzo blocco, e così via, fino a che risulterà un ultimo blocco cifrato, di lunghezza n prefissata, che sarà la firma digitale.

Quelli appena descritti sono algoritmi di facile comprensione, efficaci per dare un'idea della crittografia e dei suoi problemi. Naturalmente, gli algoritmi usati

nella pratica sono ben più complicati, perché basati su studi matematici molto raffinati, e adatti più ai matematici e agli analisti che ai giuristi: non è compito del giurista conoscere a fondo questi meccanismi né tantomeno crearne di nuovi; al giurista (informatico) è sufficiente (ma necessaria!) la conoscenza sintetica di tali fenomeni: capirne il funzionamento per poter fare applicazioni consapevoli nel campo del diritto.

(c) Dall'algoritmo bisogna tener distinta la chiave crittografica: si tratta di due concetti diversi, che però talora sono stati confusi. La chiave crittografica è un codice digitale (cioè un insieme di caratteri alfanumerici) utilizzato (da un apposito algoritmo) per cifrare e firmare (nonché decifrare e verificare) testi (messaggi, atti, etc.).

Abbiamo visto che nell'algoritmo delle *additive ciphers*, la chiave ere costituita semplicemente dal numero 3. Tuttavia, per una maggiore sicurezza, negli algoritmi più complicati anche la chiave ha una struttura più complessa. La chiave, dunque, come la firma digitale, è un codice alfanumerico. Un esempio di chiave crittografica è:

——BEGIN PGP PUBLIC KEY BLOCK——
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>

mQGiBDYbUacRBADIwqqcAaG24ANLrhxtl43Y644iqA5KbTqbRtB2VZsLWy6RpSdq
Vama+WNBGdpsOAnFEUCwCjo3qIW0+/xufkGF6uKaFDX605G4x82CToBnt9SCCVIu
NH1Hy3cJdNIRk+4EEQPs4H3w2nSFtJOWv8SaTR0PH/jAa5kiVjiTQ7vw8QCg/yS4
y04F+Wx+ujS61IfdLKPKxWkD/1yYWgO04rFbNULC2cgCk0eGURS81+nNpQkrisJ7
P5IFCnzsbG2SB/fqo4sTz6R09hgcW1+u1vE5Nw6QX58S6XAIQdKCKvVUUa4RDGCa
n/QLye4hk8Q0R6NtCOTWCqE87ywE7SNI9+4jg21B3PO76OJCP0y9OoiLrfV1yuH1
JWDdBACtPhsvWzfN5PNrErFRN70OkeuXySqg1P7nm+dF+9E7dnJ6N5s0dVCbLKWn
bc5uWF3mZRhN+WZ3MnHfNO93xNq+kWRoqLwPg1IIaEhD8ZXJUGJvU0d4T/OzaFON
QZs9mM+aUPhCPTGto6OKvH6IbYTiDSvNZZ0Fj/yx9Zb2Uk4WzLQjYWxleCBtYXR1
cm8gPGxhYm1hdEBpYm1wZS51bmljaC5pdD6JAFEEEBECABEFAjYbUacFCQB77QAE
CwMCAQAKCRDUKe37ihqMJ6DkAJ9jzBHdFVbF4tBpHEMky8vxju48zgCglDBgcrcn
QbV6R/+kYEGec+VdkK+5Ag0ENhtRpxAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+2
8W65Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZS
Tz09jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI6
1Brwv0YAWCvi9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/Cl
WxiNjrtVjLhdONM0/XwXV0OjHRbs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgH
KXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH/iaw
FJlSOpeVrTkFYDip4jf4PZsPuyFDzXbl15r09FsTqr56g9Mwn/pUaXV/SfjErYzr
eDNQk+DcHupIGQPEo5s6L7lptmCDIJ/KpcmB0yLjLT8FoD+KjnVssW/98F2R3ob/
9cdTnQLSIbPe1S0VbFZ5sPir0uAxAw8iltlf1CIYUUwG4k13mYutVQsrGlou0mbg
lA+uWYkLP1aDza8KeO0zHA6NIbJiUpUV3nf+maYCReGyeU0V91oheu49amuAJbCy

CrYQImvx5ixF1Epp3R+6+Pak8RljGafk67RJ3UxI3SHDzVc6uVGfnvVv7Jzynwb+
m6u1Wap7nR0/Ie2YkmGJAEwEGBECAAwFAjYbUacFCQB77QAACgkQ1Cnt+4oajCd2
HgCdGDOjjEbcFxPWOyrYeG9Gw2M2XX4AnjOI2mSl/GVuk19hJPccPJyf+Un4
=wKfo
——END PGP PUBLIC KEY BLOCK——

La differenza tra chiave e algoritmo è ormai ben chiara: l'algoritmo è una procedura, la chiave è un codice; l'algoritmo usa la chiave per generare la firma digitale. Come faccia l'algoritmo a usare la chiave è implicito in ciò che abbiamo osservato *supra sub* (b): la chiave è un dato individuale e concreto che s'inserisce nelle istruzioni generali e astratte dell'algoritmo; essa, in altri termini, individualizza e concretizza l'algoritmo: lo individualizza, perché essa appartiene ad uno ed un solo soggetto: solo così può essere generata una firma digitale che risponda al requisito della 'personalità'; lo concretizza, perché essa consiste in un dato concreto (quei determinati caratteri alfanumerici) necessario affinché l'algoritmo possa produrre la firma digitale.

Le chiavi e gli algoritmi crittografici possono essere di due generi: simmetrici e asimmetrici.

I) Quando si usa un sistema di chiavi simmetriche, la chiave usata per firmare il documento è uguale a quella usata per decifrare la firma; ne consegue che gli algoritmi (rispettivamente, di cifratura e decifratura) sono simmetrici: uno opera in un senso, per cifrare, l'altro opera in senso opposto, per decifrare; così, nell'esempio delle *additive ciphers*, la chiave non cambia (è sempre il numero 3), mentre gli algoritmi sono simmetrici: per cifrare, si sostituisce la lettera con la terza successiva; per decifrare, si sostituisce la lettera con la terza precedente.

In un sistema di chiavi simmetriche, il mittente firma con la chiave; comunica la stessa al destinatario, separatamente dal documento; questi verifica l'autenticità del messaggio con la stessa chiave.

Un tale sistema ha diversi inconvenienti: anzitutto, la chiave deve essere comunicata dal mittente al destinatario, con possibilità, quindi, di essere intercettata e usata abusivamente; in secondo luogo, chiunque voglia crittare testi con una chiave simmetrica, dovrà munirsi di tante chiavi quanti sono i soggetti con cui comunica: la proliferazione delle chiavi le renderebbe incontrollabili.

II) Questi inconvenienti sono eliminati nel sistema di chiavi asimmetriche. Qui, una chiave è usata dall'autore del documento per generare la firma digitale: è la chiave privata (*private key*), che si trova nella disponibilità del solo titolare. Un'altra chiave, diversa dalla prima ma ad essa collegata, viene usata dal destinatario del documento per decifrare la firma digitale, verificando così l'integrità e la provenienza del documento stesso: è la chiave pubblica (*public key*), messa a disposizione di chiunque la voglia conoscere, mediante pubblicazione in un *data base* consultabile *on line* (*key repository*), dove risulta associata al nome del suo titolare

La chiave privata è segreta; la chiave pubblica può essere conosciuta da chiunque: ma, a differenza di quanto accade nei sistemi crittografici simmetrici, tale conoscenza non genera abusi: la chiave pubblica senza la privata è, a questi effetti, inutile, perché la firma digitale può essere prodotta solo con la chiave privata; mentre la chiave pubblica serve appunto a verificare che il documento sia stato firmato con la chiave privata.

Non solo: viene eliminato anche l'inconveniente della proliferazione delle chiavi. In un sistema di chiavi asimmetriche, ciascuno ha una e una sola coppia di chiavi (*key pair*): la privata, di cui ha la conoscenza esclusiva; la pubblica, che può essere conosciuta da chiunque e permette, perciò, di comunicare con tutti.

Il regol. docum. elettr. adotta, giustamente, un sistema crittografico a chiavi asimmetriche, definendo queste ultime come "la coppia di chiavi crittografiche, una privata e una pubblica, correlate tre loro, da utilizzarsi nell'ambito dei sistemi di validazione e di cifratura di documenti informatici" (art. 1 lett. d)).

La chiave privata è "l'elemento della coppia di chiavi asimmetriche destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico [...]" (art. 1 lett. e)).

La chiave privata è, per regola, "destinata ad essere conosciuta soltanto dal soggetto titolare", cioè ad essere segreta. Il titolare delle chiavi deve: a) conservare con la massima diligenza la chiave privata e il dispositivo che la contiene; b) conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o che siano difettosi (art. 8 reg.tecn.).

Quella della segretezza della chiave privata è una regola inderogabile: il regolamento non ammette sistemi di *key escrow* o *key repository* e, anzi, vieta al certificatore di "rendersi depositario di chiavi private" (art. 92 lett. g)).

Non costituisce deroga, ma applicazione della regola appena vista, la possibilità del titolare della coppia di chiavi di depositare "in forma segreta" la chiave privata "presso un notaio o un altro pubblico ufficiale autorizzato" (art. 71). La forma di tale deposito è la stessa del deposito del testamento segreto (l'art. 73 richiama l'art. 605 c.c.- "formalità del testamento segreto"), in quanto realizzabile nella fattispecie:

I] registrazione della chiave privata "su qualsiasi tipo di supporto idoneo, a cura del depositante" (l'art. 72): potrebbe essere un foglio di carta o, più agevolmente, un supporto digitale (es. un *floppy disk* o un CD-ROM);

II] apposizione del sigillo all'involucro contenente il supporto, "in modo che le informazioni non possano essere lette, conosciute o estratte senza rotture o alterazioni" (art. 72, che integra e specifica l'art. 6051 c.c.);

III] redazione dell'atto di ricevimento e sua sottoscrizione da parte di notaio, depositante e testimoni (art. 6053-4 c.c.).

La *ratio* di tale deposito è duplice: da una parte, evitare gl'inconvenienti conseguenti alla perdita della chiave privata (es. si smarrisce la *password* d'accesso o si cancella il supporto dove la chiave è conservata); dall'altra, precostituire un ulteriore elemento di prova della *suitas* della chiave, per la risoluzione di eventuali controversie, laddove non bastasse la certificazione della C.A..

La chiave pubblica è "destinata ad essere pubblicata", "mediante la procedura di certificazione" (art. 81). Tale procedura vede protagonisti il titolare della coppia di chiavi e il certificatore:

I] "chiunque intende utilizzare un sistema di chiavi asimmetriche di cifratura" per formare, archiviare o trasmettere validamente documenti informatici "deve munirsi di un'idonea coppia di chiavi e renderne pubblica una" (art. 81); per far ciò si rivolge ad un certificatore;

II] il certificatore deve "identificare con certezza la persona che fa richiesta della certificazione" (art. 9 lett. a)); dopodiché rilascia e rende pubblico il certificato "avente le caratteristiche fissate col decreto di cui all'art. 3" (art. 9 lett. b)).

Il certificato ha l'essenziale funzione di garantire la "corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene" (funzione di certificazione) (art. 1 lett. h)).

Il certificato, come si può ricostruire dal sistema, contiene essenzialmente:

a) identificazione del titolare della chiave pubblica, cioè le sue generalità (art. 11 lett. d) reg.tecn.);
b) chiave pubblica (corrispondente al suo titolare) e algoritmo per la sua generazione (art. 11 lett. f) reg.tecn.);
c) periodo di validità della chiave pubblica (art. 11 lett. g) reg.tecn.);
d) termine di scadenza del certificato, non superiore a tre anni (art. 1 lett. h));
e) identificazione del certificatore (art. 11 lett. b) e c) reg.tecn.);
f) firma digitale del certificatore, applicata a tutti gli elementi sopra visti (lett. a)-e)): solo così può essere garantita l'integrità del certificato e la sua provenienza dal certificatore *de quo*.

Il certificato può contenere anche altri elementi (eventuali) come, ad esempio, l'indicazione dei poteri di rappresentanza o di titoli relativi all'attività professionale del titolare della chiave (ma ciò può avvenire solo col consenso dei soggetti ai quali le informazioni si riferiscono (artt. 92 lett. c) e 113 reg.tecn.).

La chiave pubblica è, dunque, pubblicata unitamente al certificato (art. 107) consultabile in forma telematica (art. 82).

Per ottenere il certificato, il (futuro) titolare deve rivolgersi ad un certificatore (*Certification Au-thority*), cioè un soggetto al quale è attribuita, per legge, una pubblica funzione certificativa. Quali sono questi soggetti? Quali i loro caratteri strutturali?

La *summa diviso* da farsi preliminarmente è tra settore privato e settore pubblico: la P.A., come vedremo, si autocertifica.

Nel settore privato, invece, la funzione certificativa è affidata solo a soggetti aventi certi requisiti fissati in generale dall'art. 83:

"a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;

"b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;

"c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;

"d) qualità dei processi informatici e dei relativi prodotti, sulla base di *standard* riconosciuti a livello inter-nazionale".

I soggetti in possesso di questi requisiti, per poter essere certificatori devono essere autorizzati (con licenza) dall'AIPA (arg. *ex* art. 84) ed inclusi in "apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto e aggiornato a cura dell'AIPA stessa" (art. 83).

I certificatori devono essere in possesso di una propria coppia di chiavi asimmetriche, che permette loro di firmare in modo digitale i certificati: sono le chiavi di certificazione (art. 44 lett. b) reg.tecn.). Ma chi certifica la loro chiave pubblica? Chi certifica i certificatori? Le risposte possono essere tre: o un certificatore sovraordinato o un certificatore equiparato o nessuno. Tre sono, quindi, i modelli possibili: anzitutto, un modello gerarchico, ordinato su due livelli, con le autorità di livello sovraordinato (*Root Authorities*) di emanazione pubblica, che certificano le autorità sottordinate private; in secondo luogo, un modello paritario, in cui ciascuna autorità è certificata da altra autorità; in terzo luogo, un modello "anarchico", in cui ciascuna autorità si autocertifica.

Nelle leggi e progetti di legge stranieri, prevale il primo modello.

Nel regolamento sul documento elettronico non prende posizione sul punto, mostrando di rimettere la soluzione alle "regole tecniche" *ex* art. 3. Il d.P.C.M. adotta, dunque, il terzo modello: "per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce" (art. 192 reg.tecn.). L'art. 21 reg.tecn. prevede, poi, la possibilità per i certificatori di seguire il secondo modello: "è consentito ai certificatori definire accordi di certificazione", vale a dire accordi in forza dei quali il certificatore A certifica la provenienza di una chiave di certificazione dal certificatore B.

Perché una firma digitale possa essere apposta validamente, il certificato (e con esso la chiave pubblica) dev'essere (tuttora) efficace, vale a dire non scaduto, non revocato, non sospeso (art. 104):

a) il termine di scadenza, si è visto, è pubblicato nel certificato *ex* art. 1 lett. h);
b) la revoca è l'atto con cui il certificatore rende inefficace *ex nunc* il certificato (art. 1 lett. l)).

Il certificatore è tenuto a revocare tempestivamente il certificato nei casi previsti dall'art. 92 lett. h):

I) richiesta del titolare (es. perché ha smarrito il supporto con la chiave privata);
II) richiesta del terzo dal quale derivano i poteri del titolare (es. in caso di revoca di una procura conferita dal terzo);
III) perdita del possesso della chiave (anche senza richiesta del titolare);
IV) provvedimenti dell'autorità;
V) cause limitative della capacità del titolare (es. fallimento);
VI) sospetti abusi o falsificazioni (basta il sospetto, non è necessario l'accertamento giudiziale).

La revoca dev'essere immediatamente pubblicata (art. 92 lett. i) e art.1 lett. k)), a garanzia dell'affidamento dei terzi, ed ha efficacia dal momento della pubblicazione (art. 105 II parte);

c) la sospensione è l'atto con cui il certificatore rende inefficace il certificato per un determinato periodo di tempo (art. 1 lett. m)).

La sospensione è disposta negli stessi casi previsti per la revoca e pubblicata negli stessi modi e con gli stessi effetti.

Se viene apposta una firma digitale mediante una chiave revocata, sospesa o scaduta, il documento si avrà per non firmato (art. 105 I parte).

Può accadere che con l'uso del sistema della firma digitale si cagioni un danno a taluno. Il principio generale del *neminem laedere* impone l'obbligo di risarcimento del danno. Ma quale sarà la natura giuridica di tale responsabilità? Sul punto il regolamento è molto rigoroso: l'art. 91 stabilisce che chiunque, utente o certificatore, "intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale è tenuto ad adottare tutte le misure organizzative e tecniche idonce ad evitare danno ad altri". È una formulazione che non lascia adito a dubbi: si tratta di una responsabilità oggettiva. La formula è quella tipica usata dal codice civile per i casi di responsabilità oggettiva, come la responsabilità per danno derivante da attività pericolose *ex* art. 2050 c.c.. Per sottrarsi a tale responsabilità, l'utente dovrà provare l'inesistenza del nesso di causalità (umana): era umanamente impossibile, allo stato della tecnologia, predisporre misure idonee ad evitare quel danno.

Si è detto che la firma digitale è l'unico strumento ritenuto idoneo a sostituire la tradizionale sottoscrizione; e si è detto pure che ciò dipende da un'affinità funzionale tra le due 'firme', pur nella loro assoluta diversità strutturale.

A) Quanto alla funzione di garantire la provenienza soggettiva (imputazione del documento), essa si specifica anche per la firma digitale in:

a) funzione indicativa: sulla firma digitale è contenuto un codice numerico che può essere rinvenuto in un *key repository* di chiavi certificate e che permette di risalire al certificato e quindi al nome del titolare della chiave pubblica;
b) funzione dichiarativa: chi genera una firma digitale, come chi appone una sottoscrizione, dichiara di assumere la paternità del documento. Ed anche nel generare una firma digitale, come nell'apporre una sottoscrizione, si pone un'esigenza di ponderatezza, tradizionalmente garantita dalla forma solenne (atto pubblico - scrittura privata) dell'atto da compiere. Tale esigenza può essere soddisfatta con particolari strumenti informatici: condizionare gli accessi alle chiavi private all'inserimento di codici segreti (*passwords*) o al riconoscimento di dati biometrici (impronta digitale, retina, etc.); o, ancora, concepire programmi di gestione delle firme digitali in modo che avvertano, mediante schermate di "attenzione!", il 'sottoscrittore' circa l'importanza dell'atto che intende compiere
c) funzione probatoria: la firma digitale apposta al documento elettronico fa prova della provenienza soggettiva del documento stesso; infatti, l'unico ad avere la disponibilità della chiave privata è il 'sottoscrittore': di conseguenza, è l'unico a poter apporre la firma digitale; la sua identità, come visto *sub* a), sarà rivelata consultando il *key repository*. Sotto questo profilo, anche il documento elettronico risponde alle esigenze di certezza e conoscibilità (mediante pubblicità) soddisfatte dalla documentazione tradizionale: il documento elettronico fa prova dell'atto documentato (prova sicura perché il documento non può essere agevolmente alterato) e può essere reso pubblico con strumenti idonei.

B) Quanto ai requisiti strutturali, la firma digitale differisce di regola dalla sottoscrizione, pur avendo con essa dei punti in comune:
a) forma scritta: quella cartacea e quella elettronica sono entrambe forme scritte; il discorso vale per la forma dell'atto, ma anche ovviamente per quella della firma;
b) autografia: solo la sottoscrizione è propriamente autografa. Tuttavia la funzione specifica di tale requisito (assicurare la provenienza esclusiva dal sottoscrittore) è soddisfatta dalla firma digitale: la chiave privata, infatti, è nella disponibilità esclusiva del titolare;
c) nominatività: la sottoscrizione è formata da prenome e cognome del sottoscrittore; la firma digitale ha un contenuto più complesso, che permette però, come si è visto, di risalire al titolare della chiave privata (il 'sottoscrittore');
d) leggibilità: requisito del tutto assente nella firma digitale, formata grazie ad una chiave crittografica;
e) riconoscibilità: pur mancando la leggibilità della firma e pur atteggiandosi diversamente dal solito il requisito dell'autografia, la firma digitale permette comunque di risalire al suo autore, nei modi visti subito *retro*;
f) apposizione in calce al documento: può esserci o meno, secondo quanto visto *retro*. Ed è per questa ragione che non di 'sottoscrizione' si parla, ma di 'firma';

g) non riutilizzabilità: la sottoscrizione tradizionale non è riutilizzabile perché fissata nel supporto cartaceo. Anche la firma digitale non è riutilizzabile, ma per un'altra ragione: il suo contenuto dipende dal contenuto del documento; se cambia il documento, deve cambiare anche la firma; se la firma venisse copiata ed apposta ad altro documento, l'applicazione della chiave pubblica e la conseguente verifica (validazione) svelerebbero subito l'abuso. Della firma digitale si può abusare efficacemente solo possedendo la chiave privata.

Nella non riutilizzabilità consiste, come si è visto, la differenza fondamentale (e decisiva ai fini di una scelta tra le alternative) tra firma digitale e firme biometriche (ivi compresa la 'sottoscrizione elettronica').

Abbiamo finora parlato dell'uso della crittografia per garantire l'integrità e la provenienza di un documento elettronico, con lo strumento della firma digitale.

Ma la crittografia può essere utilizzata anche ad altri scopi, e segnatamente allo scopo, che rinvia alle sue origini remote, di garantire la segretezza delle comunicazioni.

Per rendere segreto un messaggio, non basta firmarlo digitalmente: la firma digitale non fa che aggiungersi al messaggio 'in chiaro' (*plaintext*); il messaggio potrà essere intercettato e letto, anche se non potrà essere alterato.

Per cifrare il messaggio)si usa, nel sistema crittografico a chiavi asimmetriche, la chiave pubblica del destinatario: il messaggio così crittografato (c.d. *digital envelope*: una specie di 'busta digitale' chiusa e sigillata inviata al destinatario) potrà essere decifrato e letto solo dal destinatario applicando la propria chiave privata.

Il fenomeno coinvolge due ordini di valori (e di correlati interessi) confliggenti: da un lato, il principio per cui "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili" (art. 151 Cost.); dall'altro, l'interesse pubblico alla sicurezza e all'ordine, che possono essere pregiudicati se le comunicazioni segrete mirano a scopi eversivi. Come trovare un punto d'equilibrio tra le due opposte esigenze? È possibile trovarlo o bisogna far prevalere necessariamente l'una o l'altra?

Il problema ha dimensioni planetarie; è emblematica la storia di Philip Zimermann, programmatore americano, ideatore di PGP, programma che serve a crittografare messaggi elettronici: egli, sostenitore dell'inviolabilità della comunicazione libera e segreta, ha messo a disposizione il suo PGP sulla rete *Internet*, sicché chiunque (anch'io l'ho fatto!) può prelevarlo, 'scaricandolo' sul proprio *computer*; per questa ragione, è stato accusato dal Governo degli Stati Uniti di esportazione illegale di armi pericolose ("PGP è pericoloso come una bomba!"): il programma può essere usato anche da terroristi e criminali per sottrarre le proprie comunicazioni alle intercettazioni delle forze dell'ordine.

Consapevoli di questi problemi, anche in Italia ci si è posti difronte all'alternativa: libertà o controllo?

Le principali forme di controllo sono due: il *key escrow* e il *key recovery*. La prima consiste nell'affidare una copia della chiave privata ad una *Trusted Third Party* autorizzata; la seconda, nota anche come *backdoor*, consiste nel lasciare un 'passag-

gio segreto' aperto negli algoritmi crittografici, tale da permettere alle *TTPs* di ricostruire, su richiesta, le chiavi private. Entrambi gli strumenti permettono all'autorità di polizia di intercettare e leggere la corrispondenza delle organizzazioni criminali; ma a farne le spese potrebbero essere anche i comuni cittadini: il *key escrow* e "la *backdoor* possono costituire realmente l'arma risolutiva del Grande Fratello digitale, impugnata con il pretesto della lotta alla criminalità".

E allora, che fare? Un sistema potrebbe essere il seguente: dato che la 'rottura' di una chiave crittografica è solo una questione di potenza di calcolo, si potrebbe costituire un solo grande centro di calcolo (magari a livello internazionale), che sia in grado di decrittare in tempi ragionevoli i messaggi crittografati. Tale procedura dovrebbe essere attivata solo "per atto motivato dell'autorità giudiziaria, con le garanzie stabilite dalla legge", come richiesto dall'art. 152 Cost..

Il primo schema di regolamento sul documento elettronico (diffuso nel settembre 1996) prevedeva un sistema di *key escrow*. Il testo definitivo del regolamento (10 novembre 1997) non prevede più quell'istituto, ma stabilisce, al contrario, che la chiave privata è "desinat[a] ad essere conosciut[a] soltanto dal soggetto titolare" (art.1 lett. e)) e che "il certificatore è tenuto a [...] non rendersi depositario della chiave privata", cioè a non assumere il ruolo di *TTP* (art.92 lett. g)). Si è scelta, dunque, la via della libertà e segretezza della corrispondenza e della più intensa tutela della *privacy*.

La tutela della *privacy* è anche lo scopo dell'art. 3 regol. docum. elettr., posto a garanzia della "segretezza della corrispondenza trasmessa per via telematica": "1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.)Agli effetti del presente regolamento, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario".