L'evoluzione del progetto dell'AIPA

TROPPA BUROCRAZIA PER IL DOCUMENTO DIGITALE

Il progetto dell'Autorità per l'informatica nella pubblica amministrazione, del quale abbiamo già parlato sul numero del mese scorso, è partito col piede giusto: la bozza pubblicata su Internet, con l'invito a intervenire ed esprimere osservazioni e proposte. Ecco le nostre, che riguardano soprattutto gli aspetti burocratici.

di Manlio Cammarata

In Italia di solito le leggi nascono in gran segreto, elaborate nelle segrete stanze dei ministeri da burocrati che spesso conoscono troppo bene gli arcani percorsi dell'amministrazione, mentre ignorano molti aspetti della realtà con la quale le norme dovranno essere confrontate. Ai cittadini giungono indiscrezioni più o meno pilotate, frammenti di notizie, titoli di giornali più attenti all'effetto che alla sostanza dell'informazione. Con il progetto «Atti e documenti in forma elettronica», l'Autorità per l'informatica nella pubblica amministrazione rompe questa inveterata abitudine e accetta, in parte, la logica aperta della Rete, fatta di confronto e di trasparenza. In parte, perché offre a tutti la possibilità di esprimere un'opinione, ma poi non pubblica i testi ricevuti e quindi non stimola la discussione. Cerchiamo di farlo noi, con un'apposita pagina nella «Attualità» del Forum multimediale «La società dell'informazione», nella quale pubblichiamo le nostre osservazioni e quelle di tutti coloro che vorranno intervenire.

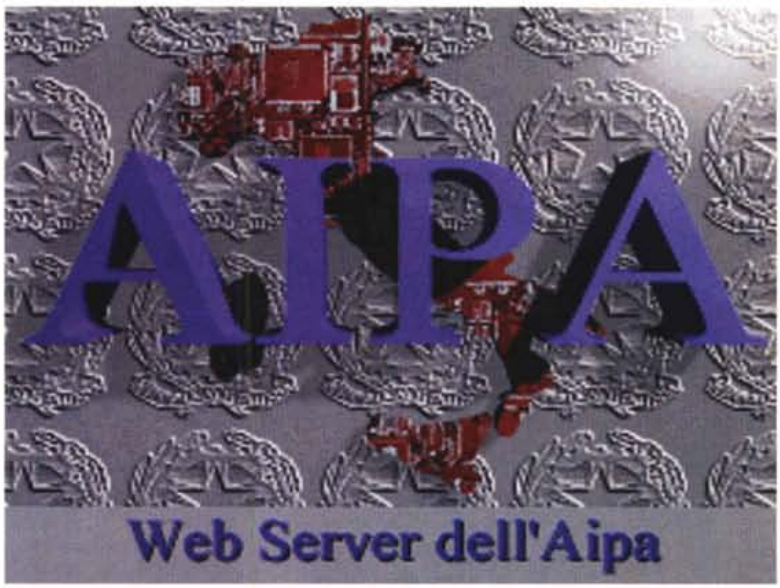
Il testo dell'Autorità è alla URL **<http://www.aipa.it/notaria/notaria.htm>**, mentre la nostra pagina è **<http://www.mclink.it/inforum/docdigit.htm>**.

L'argomento si presta particolarmente bene alla discussione telematica, perché riguarda proprio le informazioni digitali, il modo in cui si creano, si archiviano si trasmettono a distanza, e soprattutto le procedure che trasformano le informazioni in «documenti» in senso legale.

Il passaggio dal documento cartaceo a quello digitale è un passaggio obbligato verso la società dell'informazione, sia per la pubblica amministrazione, sia per i rapporti privati, perché consente di smaterializzare l'informazione svincolandola dal supporto. In questo modo si ottiene una sorta di «informazione pura», solo «contenuto», che può di volta in volta essere messo sulla carta o su un supporto informatico, o trasmesso dovunque in tempo reale.

Il documento digitale è anche e soprattutto l'elemento essenziale per realizzare la rete della pubblica amministrazione (ne parla Leo Sorge nel riquadro): gli uffici pubblici si devono scambiare non solo semplici informazioni, ma soprattutto «documenti», cioè informazioni di contenuto certo e immodificabile, attribuibili a soggetti ben identificati. Questo è appunto l'oggetto della bozza di legge che l'AIPA sta elaborando.

Scrittura, documento, atto



Il CERT-IT (Computer Emergency Response Team Italiano) ha pubblicato una nota molto critica sul progetto dell'AIPA. Si trova su ***<http://idea.sec.dsi.unimi.it/attiedoc.html>***.

Per inquadrare bene i termini della discussione è necessario mettere a fuoco il concetto di «documento», cioè dell'informazione che presenta requisiti che le conferiscono determinati effetti legali. Il termine normalmente usato dai legulei è «scrittura», che la definiscono come «rappresentazione della realtà», ed è evidentemente legato alla tradizione cartacea. La scrittura può essere di diversi tipi (per esempio, la «scrittura privata»), ma solo in alcuni casi può essere considerata «documento» e quindi produrre certi effetti. Una scrittura (ma sarebbe bene usare il termine «informazione») è un documento quando il suo contenuto è certo e immodificabile e può essere attribuita a un determinato soggetto. In pratica si tratta di un supporto cartaceo, scritto a mano o con mezzi meccanici (ma in modo che non si possa cancellare o che si possano notare le tracce di un'eventuale cancellazione) e «sottoscritto», cioè firmato da un soggetto e, in qualche caso, munito anche di un timbro o sigillo. Non si deve dimenticare che parte essenziale di un documento è la data della sua formazione e spesso anche quella della sua consegna al destinatario. Documenti di particolare efficacia probatoria possono anche essere redatti su carta apposita, contraddistinta da un disegno particolare o da una filigrana, e spesso anche «vidimati», cioè provvisti di indicazioni che vengono apposte da soggetti a ciò designati, che testimoniano in genere il momento a partire dal quale le scritture sono valide per i fini previsti dalle norme.

Tutto questo è necessario per conferire ai documenti la certezza delle informazioni che contengono, sia a scopi semplicemente «certificatori», sia come mezzo di prova nei processi civili e penali. Una specie particolare di documenti è costituita dagli «atti»: si tratta di documenti redatti da determinati soggetti (pubbliche amministrazioni, o pubblici ufficiali) con determinati requisiti formali, che hanno un particolare valore legale. Pensiamo a un atto di vendita di un immobile, redatto da un notaio, o a una multa per un'infrazione al codice della strada. Ma stiamo parlando di scritture su carta. Come la mettiamo con i bit? I bit sono uno uguale all'altro, la copia è sempre identica all'originale, l'alterazione non lascia tracce, la falsificazione è facilissima. Occorre un sistema per «certificare» i bit, per far sì che si possa avere la certezza che una «scrittura digitale» è stata composta in un determinato momento, da un determinato soggetto e che il suo contenuto non sia stato modificato. Dal punto di vista giuridico la questione non è semplice, e alcune norme degli ultimi anni non hanno modificato la sostanza del problema: c'è l'art. 3 del Dlgs 39/93 (quello che ha istituito l'AIPA) e ci sono alcune disposizioni della legge 547/93, che adatta al crimine informatico il codice penale e il codice di procedura penale. Nell'art. 3 del Dlgs 39/93 si legge: *1. Gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite i sistemi informativi automatizzati. 2. Nell'ambito delle pubbliche amministrazioni l'immissione, la riproduzio-*

ne su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante sistemi informatici o telematici, nonché l'emanazione di atti amministrativi attraverso i medesimi sistemi, devono essere accompagnate dall'indicazione della fonte e del responsabile dell'immissione, riproduzione, trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile. È evidente che queste disposizioni non sono sufficienti a configurare il documento digitale, servono solo ad assicurare l'efficacia di documenti cartacei formati con sistemi informatici. E infatti l'art. 22 della bozza dell'AIPA recita: *Il primo comma dell'art. 3 del Decreto Legislativo 12 febbraio 1993 n. 39 è sostituito dal seguente: «Tutti gli atti, i provvedimenti, i procedimenti ed i documenti in genere, in qualsiasi stato e grado formulati e posti in essere dalle pubbliche amministrazioni sono di norma predisposti con l'ausilio di sistemi informativi automatizzati e conservati su supporto informatico o altro supporto a tecnologia avanzata avente caratteristiche di non riscrivibilità ed inalterabilità nel tempo.» Nel secondo comma dell' art. 3 del Decreto Legislativo 12 febbraio 1993 n. 39, le parole «dall'indicazione a stampa» sono sostituite dalle parole «dal contrassegno elettronico».*

Vediamo ora le norme del codice penale sui crimini informatici: *Art. 491-bis. – (Documenti informatici). – Se alcuna delle falsità; previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.* C'è un errore concettuale, ancora legato alla cultura del documento cartaceo, perché l'efficacia probatoria può anche non essere nel «supporto», dal momento che l'informazione digitale può essere facilmente trasportata da un supporto all'altro. E manca ancora l'idea dei requisiti che possono conferire efficacia probatoria al documento informatico, che invece troviamo nella bozza di articolato predisposta dall'AIPA. Qui si capisce come gli elementi che conferiscono efficacia al documento debbano essere «incorporati» nell'informazione e non nel supporto. A questo proposito è necessario che nel testo finale sia inserita una più chiara distinzione tra il supporto e le informazioni che esso contiene, abbandonando qualsiasi paragone con il documento cartaceo: questo non deve essere preso come modello, ma soltanto come una delle possibili forme che può assumere un documento.

Ma nei nuovi articoli del codice penale, introdotti dalla legge 547, ci sono altri punti che possono generare problemi a non finire: la confusione, nello stesso articolo 491-bis, tra i documenti e i programmi destinati a elaborarli, mentre nel secondo comma dell'art. 621 torna l'equivoco tra supporto e contenuto: *Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi (il primo comma dice: Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio*

Pochi soldi per la Rete della PA

di Leo Sorge

Con 1050 miliardi in tre anni si connetterebbe la PA, dice l'Autorità. Il Governo le crede, ma stanzia solo 180 miliardi. Di cui trenta subito

La ciclopica legge finanziaria '97 prevede anche le fondamenta di una rete unitaria o rete di reti, con gli standard di Internet, della PA italiana. Sulla scorta d'un progetto dell'AIPA divenuto disegno di legge e definitivamente approvato dal Senato il 14 novembre scorso, il Governo ha stanziato 30 miliardi già nel 1996, 50 per il '97 e 100 per il '98.

Il progetto viene definito compatibile con le leggi italiane e le direttive comunitarie che nel corso degli anni hanno affrontato aspetti di questo stesso problema, tra le quali la L. 241/90 sul procedimento amministrativo, e il progetto comunitario IDA - Interchange Data between Administration. Secondo l'AIPA i costi da sostenere sarebbero di 350 miliardi l'anno per tre anni, corrispondenti ad un incremento del 10% del capitolo di spesa.

Tre le aree di intervento: instradamento dei dati, interoperabilità e omogeneità delle applicazioni. Tecnicamente si prevede una rete metropolitana a larga banda per l'area di Roma prima e per Milano a seguire, entrambe già tracciate con progetti di massima, oltre alla ovvia interconnessione con la rete scientifica GARR. Nel progetto non si parla esplicitamente di reti civiche, ma si dettaglia l'adesione di Regioni ed altri enti locali tramite l'ANCI (Associazione dei Comuni) che offre servizi telematici. Il coordinamento sarà affidato al Ministero dell'Interno. Per il valore che possono avere, le statistiche valutano al 15% l'attuale informatizzazione della nostra PA, per di più con costi di gestione spropositati. Obiettivo della rete unitaria è portare tale valore al 60% entro l'anno 2000, al contempo migliorando l'efficienza e riducendo gli sprechi.

Va segnalato che restano irrisolti i problemi di quota più elevata quali il televoto, il telepagamento o la firma elettronica, rimandati a futuri lavori legislativi. Ma l'AIPA se ne sta occupando, come si legge in queste pagine.

o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da lire duecentomila a due milioni). Molte altre sono le norme del nostro sistema legislativo che devono essere riviste alla luce della futura legge sul documento digitale, e sarebbe forse opportuno inserire una norma di carattere generale che stabilisca l'efficacia della sottoscrizione digitale per qualsiasi documento, annullando esplicitamente ogni disposizione incompatibile. Molte disposizioni devono essere riscritte da zero, come quelle sulla «protocollazione» dei documenti: quando questi sono trasmessi per via telematica, il «protocollo» è del tutto automatico e si realizza in tempo reale.

Tecnica di una rivoluzione

Dunque il problema è come incorporare nell'informazione gli elementi che possono qualificarla come documento. La risposta è nella tecnologia digitale, che mette a nostra disposizione gli algoritmi di cifratura a chiave asimmetrica, dei quali ha parlato Corrado Giustozzi un mese fa in queste pagine. Essi consentono di codificare una «scrittura» in modo che si possa accertare, con un margine di sicurezza pressoché assoluto, sia l'autenticità del contenuto, sia l'identità del soggetto che ha predisposto il documento. Il procedimento è semplicissimo e viene compiuto dall'elaboratore in pochi istanti: da una parte c'è l'informazione sotto forma di bit, dall'altra l'algoritmo di cifratura, anch'esso digitale e composto da due «chiavi», una pubblica (cioè conoscibile da chiunque) e una privata, che deve essere tenuta segreta dal suo titolare. Il sistema «frulla» insieme l'informazione e la chiave pubblica del destinatario e produce una sequenza di bit assolutamente incomprensibile. Il computer destinatario del documento prende questi bit, li «frulla» con la chiave privata e riproduce le informazioni originarie. Questo procedimento serve soprattutto per la cifratura dei documenti, cioè per rendere il loro contenuto intelligibile solo al destinatario, e per questo l'operazione è fondata sull'uso della chiave pubblica del destinatario stesso.

Tuttavia nella pubblica amministrazione e nelle transazioni commerciali il problema non è tanto la segretezza delle informazioni, quanto la loro autenticità, cioè la garanzia che provengano da un determinato soggetto e che non siano state alterate dopo la formazione o la trasmissione del documento. Gli algoritmi a chiave asimmetrica rispondono perfettamente a questa esigenza, perché funzionano anche al contrario: il mittente «frulla» le sue informazioni con la propria chiave privata e il destinatario le decifra con la chiave pubblica del mittente (nel caso precedente, invece, il mittente usa la chiave pubblica del destinatario).

Siccome nel «frullato» possono essere compresi anche i dati che identificano il mittente e altre indicazioni, come la data e l'ora di composizione della scrittura, l'insieme si «autocertifica»: qualsiasi alterazione dei bit dopo la cifratura rende impossibile l'operazione inversa. Se il documento viene decifrato con la chiave privata del mittente, vuol dire che è stato proprio lui a produrlo. Questa certificazione è molto più sicura di quella basata sulla firma autografa, e sui timbri, perché firme e timbri possono essere falsificati con una certa facilità, mentre la stringa di bit che compone una chiave privata non è riproducibile a partire da quella pubblica.

Resta un solo punto oscuro: come possiamo avere la certezza che una chiave pubblica appartenga a un determinato soggetto? Per capire il problema, facciamo un esempio: Tizio deve inviare a Caio una dichiarazione di particolare importanza, e lo fa con un messaggio di posta elettronica cifrato con la propria chiave privata. Caio decifra il messaggio con la chiave pubblica di Tizio, che ha

Niente balzelli

Nella bozza predisposta dall'Autorità per l'informatica nella pubblica amministrazione ci sono alcuni aspetti che è opportuno sottolineare. Secondo l'art. 23 *Le copie di atti pubblici, scritture private e documenti in genere, in essi compresi gli atti e documenti amministrativi di ogni tipo, comunque formati o riprodotti in forma di documento elettronico, spedite dai pubblici depositari autorizzati e dai pubblici ufficiali di cui agli art. 2714 e 2715 codice civile, hanno la stessa efficacia delle copie realizzate su supporto cartaceo se munite del contrassegno elettronico, certificato autentico dalla A.N.C. e dal C.S.A.C., di colui che le spedisce. Esse sono in modo assoluto esenti da imposte di bollo e T.C.G.* Dunque il documento digitale dovrebbe essere esente da tutti i balzelli che vengono imposti ai cittadini per ogni atto amministrativo. Resta un piccolo dubbio: solo «le copie» o anche gli originali degli atti?
Un altro punto interessante concerne la natura del contrassegno «elettronico» (art. 7): *Nei modi e con le tecniche che verranno definiti in seno all'emanando Regolamento, dal contrassegno elettronico dovranno sempre potersi rilevare: per le persone fisiche: cognome, nome, luogo e la data di nascita, domicilio e codice fiscale – per i soggetti diversi dalle persone fisiche: denominazione, sede del soggetto o ente titolare, codice fiscale; cognome, nome, luogo e data di nascita e rapporto funzionale o di rappresentanza della persona fisica consegnataria – la data di sua generazione a cura della competente Autorità di certificazione – il periodo iniziale e finale di sua validità – l'orario di apposizione al documento o al gruppo di documenti cui si riferisce l'eventuale certificazione di sua validità, a norma della presente legge.* È facile immaginare quali semplificazioni potranno derivare da un'applicazione generalizzata di questa «carta d'identità virtuale», anche nell'uso combinato con le «carte intelligenti» che finalmente incominciano a diffondersi per gli usi più disparati.

ricevuto in precedenza... ma è stato proprio Tizio a mandargliela, o è stato Sempronio che cerca di farsi passare per Tizio? La risposta è nella «certificazione» della chiave pubblica di Tizio. In pratica Caio deve poter consultare un elenco di chiavi pubbliche, tenuto da un apposito ente di certificazione, dal quale risulti che quella chiave appartiene proprio a Tizio e non a un altro. Facciamo un altro esempio: un ufficiale di polizia giudiziaria riceve per via telematica l'ordine cifrato di arrestare una persona.

L'ordine, naturalmente, proviene da un magistrato, che lo ha cifrato due volte, prima con la chiave pubblica dell'ufficiale giudiziario (per renderne segreto e immodificabile il contenuto), poi con la propria chiave privata (per certificarne la provenienza). L'ufficiale decifra il messaggio con la propria chiave privata, poi con la chiave pubblica del magistrato, così è sicuro che non proviene da un buontempone in vena di scherzi di cattivo gusto. Ma questa sicurezza è tale solo se la chiave pubblica del magistrato è compresa in un elenco di chiavi certificate, che costituisce il cuore del sistema. Questo esempio rende l'idea di quale rivoluzione possa essere innescata dall'uso del documento digitale: se quel testo compare su un giornale, come oggi accade troppo speso, o lo ha fatto trapelare il mittente, o lo ha fatto trapelare il destinatario. E si può conoscere passo dopo passo il percorso seguito dal documento e il tempo impiegato (addio, vecchio «protocollo» burocratico, la prima causa della lentezza delle pratiche!), si può avere una «ricevuta di ritorno» completamente automatica, si può seguire tutto l'iter di una procedura, registrato automaticamente se la procedura stessa è svolta con sistemi informatici. Addio file agli sportelli, addio certificati, addio «dottori fuori stanza», addio fascicoli che scompaiono e riappaiono in luoghi improbabili (ma al momento giusto!), addio *dossier* pieni di notizie compromettenti, che non si sa chi ce le ha messe, e mancanti di altre informazioni, che non si sa chi le ha tolte. Possiamo sognare che tra pochi anni una nuova legge modifichi quella oggi in preparazione e dica più o meno: dal tale giorno è vietata la carta!

Ma cerchiamo di capire meglio il meccanismo della certificazione delle chiavi. Partiamo dall'ipotesi che esista già un registro pubblico delle chiavi certificate, costituito da un computer collegato a Internet (e quindi consultabile da chiunque) e provvisto di opportuni sistemi di sicurezza, e vediamo come potrebbe svolgersi la procedura di assegnazione di una chiave certificata al signor Rossi. Il signor Rossi si reca da un notaio, o da un segretario comunale o da un altro pubblico ufficia-

I seminari del Forum multimediale: si replica

Molti partecipanti, grande interesse e un consenso generale che viene dalle cifre: questo il bilancio dei primi due seminari del Forum multimediale «La società dell'informazione», organizzati in collaborazione con la scuola di management della Luiss Guido Carli, che si sono tenuti a Roma il 28 e 29 novembre scorso.

Un momento dei seminari «Le leggi di Internet».

Quaranta iscritti alla prima giornata, quarantadue alla seconda (trentatré hanno seguito le due giornate), 15 ore effettive di lavori con la partecipazione di 12 relatori; le schede di valutazione restituite alla fine della prima giornata sono state 39, 25 alla fine della seconda. L'elaborazione delle risposte ha dato questi risultati:

– una totale soddisfazione nei confronti dell'iniziativa
– una totale soddisfazione verso il contenuto del seminario, la qualità dei relatori e la scelta dei temi
– la percezione che sia l'iniziativa sia i contenuti hanno un diretto risvolto di utilità professionale
– si desidererebbe tuttavia una trattazione più ampia e completa dei temi proposti

I dettagli sono, naturalmente, nel Forum multimediale, **<http://www.mclink.it/inforum/seminar1.htm>** alla voce «Seminari» della home page.

A questo punto non resta che mettersi al lavoro per preparare nuovi incontri. Replicheremo i temi già trattati, per chi non ha potuto partecipare alla prima edizione, e tratteremo anche nuovi argomenti di grande attualità. Gli aggiornamenti, naturalmente, saranno tempestivamente pubblicati nel Forum, oltre che su queste pagine.

Un mezzo di prova

Il contrassegno digitale applicato a una scrittura la trasforma in un documento opponibile a terzi e con il valore probatorio stabilito dagli artt. 8, 9 e 10 della bozza dell'AIPA. Recita infatti l'art. 8: *L'applicazione del contrassegno elettronico equivale alla sottoscrizione, prevista per gli atti e documenti a forma scritta su supporto cartaceo, del documento elettronico cui esso è apposto.*
Il documento elettronico sottoscritto con contrassegno elettronico è opponibile al suo sottoscrittore, tranne che quest'ultimo non dimostri di aver segnalato alla Autorità Certificatrice, in un momento anteriore a quello della sottoscrizione, l'avvenuto uso fraudolento o l'avvenuta sottrazione o alterazione della propria chiave segreta di criptazione.
L'uso di contrassegno elettronico revocato equivale a mancata sottoscrizione, tranne che il suo titolare non ne confermi nel caso specifico l'autenticità e validità, fatti salvi i diritti dei terzi ed eventuali ipotesi di reato.
Degli aspetti contrattuali si occupano gli articoli successivi. L'art. 9 stabilisce: *Il documento elettronico si intende pervenuto al destinatario nel domicilio da questi dichiarato alla competente Autorità di cui all'art. 11 risultante dal certificato rilasciato al richiedente dall'Autorità emittente e pubblicato nell'elenco delle chiavi pubbliche di cui agli articoli 25 e segg. della presente legge. Mentre l'art. 10 determina il meccanismo della «ricevuta di ritorno» digitale: La data e l'ora, sia di spedizione sia di ricezione, del documento elettronico redatto con le caratteristiche di cui alla presente legge ed al suo regolamento di attuazione sono opponibili alla controparte ed ai terzi, tranne prova contraria, ove per la trasmissione si sia fatto uso di sistema informatico preposto alla generazione ed all'invio di una attestazione automatica di avvenute trasmissione e ricezione, avente i requisiti di idoneità individuati dal Regolamento di attuazione e periodicamente certificato idoneo dal C.S.A.C. – Consiglio Superiore delle Autorità di Certificazione, di cui al successivo art. 11, nei modi e termini di cui al Regolamento medesimo.*

le (per esempio, il comandante della stazione dei carabinieri di un piccolo centro) e chiede l'assegnazione di una chiave di crittografia. Il pubblico ufficiale si accerta dell'identità del richiedente e quindi, con il suo PC, genera la coppia di chiavi, con una procedura che gli rende invisibile la chiave privata, che consegna all'interessato (presumibilmente su un dischetto che il signor Rossi ha avuto cura di portare con sé). Quindi, dato che anche il suo PC è collegato alla rete della PA, invia la chiave pubblica dell'interessato al registro pubblico, con un messaggio cifrato con la chiave pubblica del registro stesso e con la propria chiave privata. Il computer del registro pubblico verifica automaticamente il tutto (se no, che computer sarebbe?) e inserisce nell'elenco la chiave pubblica del signor Rossi. Tutto qui.

Per quanto riguarda le chiavi delle istituzioni e della pubblica amministrazione, basta istituire presso gli enti più importanti su base funzionale o territoriale appositi uffici per la generazione e la trasmissione delle chiavi al registro. Naturalmente occorre qualcuno che eserciti un certo controllo su tutto il meccanismo, più a fini organizzativi che di verifica.

Non servono tanti controlli a priori o a posteriori, perché il sistema, se ben costruito, si verifica da sé con l'uso incrociato delle chiavi pubbliche dei mittenti e dei destinatari. Gli imbrogli sono praticamente impossibili: come si fa, per esempio, a retrodatare un documento digitale, se tutti i computer attraverso i quali passa quel documento pongono il loro «timbro» digitale sul documento stesso (vedi la posta elettronica su Internet)? Ma qui scatta la trappola infernale della burocrazia.

La burocrazia con le maiuscole

La bozza di articolato predisposta dall'AIPA presenta aspetti positivi e negativi. Il dato positivo più importante è l'aver colto in pieno la natura e i vantaggi della documentazione digitale e averne previsto gli effetti, ponendo le premesse per quella «svolta epocale» che oggi è possibile, ma che solo pochi mesi fa sembrava folle immaginare. Il progetto è fondato su meccanismi collaudati e standardizzati, di facile adozione, perfettamente integrati nel disegno della rete unitaria della pubblica amministrazione. Questa, a sua volta, è del tutto «Internet compatibile», anzi, è un pezzo di Internet, e quindi la PA si integra nel modello nascente della società dell'informazione. Il che significa, fra l'altro, l'abbattimento di moltissimi vincoli gerarchici, che si rivelano del tutto inutili, perché nel modello Internet il funzionamento del sistema deriva dall'adesione dei singoli soggetti a un insieme di norme tecniche: chi non aderisce non entra, perché il collegamento non funziona. Non è necessario certificare che un computer della rete dispone dei necessari protocolli TCP/IP, perché se non li ha (o se contengono qualche errore) il computer non è in rete. Lo stesso discorso può valere per la certificazione delle chiavi: se non seguo la procedura automatica di generazione e comunicazione della chiave al registro pubblico, la chiave certificata non esiste!

Tutto questo è di una semplicità «spaventosa», il contrario della burocrazia.

E infatti i burosauri, appena si sono accorti della semplicità e dell'efficacia del meccanismo da loro

stessi ipotizzato, si sono affrettati a inserire una serie di norme in grado di assicurare la sopravvivenza del loro habitat, immaginando una nuova burocrazia che possa frenare l'avanzata della semplificazione. Hanno inventato il Consiglio Superiore delle Autorità di Certificazione, l'Autorità Amministrativa di Certificazione, l'Autorità Notarile di Certificazione, le Autorità Intermedie di Certificazione, le Autorità Private di Certificazione, il Registro Unico delle chiavi pubbliche di criptazione, gli Archivi delle chiavi di criptazione e forse qualche altro ente che ora mi sfugge. Un'orgia di Autorità degna di un film sulle guerre stellari, un delirio di lettere maiuscole e di sigle da scioglilingua: C.S.A.C., A.A.C., A.I.C., A.N.C., A.P.C... Che non servono a nulla, se non ad assicurare lauti stipendi e comode poltrone, oltre che a rallentare le procedure.

Se si accettano i principi della Rete e del documento digitale, il sistema può funzionare in maniera quasi del tutto automatica e con un elevato grado di sicurezza. Nell'esempio della chiave del signor Rossi, fatto nel paragrafo precedente, occorre solo che nel computer del registro pubblico ci sia il software giusto e che il maresciallo dei Carabinieri (o chi per lui) abbia un PC in rete e non la-

Le modifiche alla bozza dell'AIPA

Il testo che segue è una proposta per modificare in alcuni punti la bozza di disegno di legge dell'AIPA «Atti e documenti elettronici». Non è un articolato completo, ma prende in considerazione solo alcuni aspetti, sulla base dei quali si dovrebbe metter mano a una riscrittura, non sostanziale, di una parte del testo rimanente. La prima osservazione riguarda una questione terminologica: la definizione di «documento elettronico» non è sbagliata, ma sarebbe meglio parlare di «documento digitale», anche se in questo momento il significato della parola «digitale» non è chiaro a tutti gli italiani e, probabilmente, a buona parte dei parlamentari che dovrebbero discutere la proposta. Il punto essenziale non è nell'uso di apparecchiature elettroniche (che possono essere anche non digitali, come un televisore), ma nel fatto che il testo si riferisce a documenti rappresentati da bit, cioè documenti in formato digitale, non «elettronici», che non significa nulla. Un altro aspetto forse secondario (ma, visto che ci siamo, cerchiamo di fare le cose per bene!) riguarda i termini usati per indicare le varie fasi delle procedure. Quindi è bene parlare di «cifratura» piuttosto che di «crittografazione», termine che si riferisce al procedimento per rendere intelligibili le informazioni solo al destinatario, e non all'intero processo di autenticazione; così sarebbe bene parlare di «chiavi di cifratura» e di «contrassegno digitale» invece che di «chiavi di criptazione» o «chiavi di codifica» e di «contrassegno elettronico». E via discorrendo.
Sono particolarmente importanti le modifiche proposte per gli articoli 11 e 12, che riducono al minimo la struttura burocratica prevista nella bozza dell'AIPA. Il meccanismo «autocertificatorio» degli algoritimi a chiave asimmetrica, insieme al principio della «rete come sistema informativo», permette di eliminare le strutture intermedie: la certificazione fa capo ai soggetti certificanti, l'archivio detta le regole. Passiamo al testo, con un'ultima avvertenza: è stato seguito uno schema più lineare, mettendo prima di tutto le definizioni, quindi la modifica del quadro legislativo e poi i dettagli. Ultima pignoleria: un articolo precedente è, appunto, «precedente», non «superiore», che introduce una fuorviante idea di gerarchia.

Art. 1 - Definizioni
Ai fini di questa legge e di ogni altra disposizione applicabile, si intende per:
a) forma scritta: qualsiasi rappresentazione della realtà in forma testuale, grafica, sonora, o altra consentita dalla tecnica, registrata su qualsiasi supporto;
b) documento: qualsiasi atto o rappresentazione della realtà ai sensi della precedente lettera a), che abbia requisiti di certezza e immutabilità e possa essere attribuito a un soggetto determinato;
c) documento digitale: qualsiasi atto o documento avente i requisiti descritti alla precedente lettera b), redatto o archiviato o trasmesso con mezzi digitali;
d) cifratura: procedimento attraverso il quale un atto, documento o altra rappresentazione in forma scritta viene resa intelligibile al solo destinatario;
e) algoritmo a chiave asimmetrica: procedura di crittografia o certificazione basata sull'uso di una chiave di cifratura pubblica, alla quale corrisponde una chiave segreta di decifratura;
f) contrassegno digitale: elemento identificativo univoco di un soggetto, realizzato mediante un algoritmo a chiave asimmetrica certificato da un soggetto abilitato;
g) chiave certificata: la coppia di chiavi assegnate a un utente, generate da un soggetto a ciò autorizzato, con le procedure descritte nel successivo art. 11.

Art. 2 - Contesto legislativo
Questo articolo deve modificare l'art. 3 del decreto legislativo 39/93, la legge n. 15 del 4 gennaio 1968 e gli articoli dei codici civile e penale (in particolare quelli introdotti dalla legge 547) e dei di codici di procedura civile e penale per tutto quanto riguarda la sottoscrizione e l'efficacia probatoria dei documenti. Devono essere modificati anche i regolamenti fiscali e amministrativi, per arrivare alla completa equiparazione delle scritture cartacee e di quelle digitali.

Art. 3 - Regolamento di attuazione
Rimane il testo originale dell'art. 2.

Artt. 4, 5, 6, 7, 8, 9 , 10 - Chiavi e contrattazione con mezzi digitali
Rimane, nella sostanza, il testo originale, con le modifiche terminologiche indicate nella premessa. È necessario inserire un comma che affermi che chiunque può generare e utilizzare in proprio chiavi di cifratura per

sci in giro la sua chiave privata. Tutto qui. Per il resto il progetto dell'AIPA appare accettabile sul piano sostanziale.

Qualche appunto può essere rivolto alla forma, perché la terminologia non è sempre corretta (si veda ancora «Terminologia crittografica» di Corrado Giustozzi, in Informatica e Società del mese scorso). Occorre anche una maggiore attenzione al quadro legislativo di riferimento, perché il testo prende in considerazione, in due punti diversi, solo il codice civile e il Dlgs 39/93, mentre il documento digitale richiede una revisione a trecentosessanta gradi delle norme civili, penali e amministrative, che sarebbe opportuno riunire in un solo articolo, con l'inserimento di disposizioni di portata generale, o forse con la previsione di una delega al governo.

A questo punto non resta che accogliere l'invito dell'AIPA alla discussione e avanzare una immodesta proposta di modifica del testo, che trovate nel grande riquadro.

E, naturalmente, sfruttiamo la Rete: apriamo una pagina dedicata al documento digitale nel nostro Forum multimediale «La società dell'informazione», alla URL **<http://www.mclink.it/inforum/docdigit.htm>**.

rapporti privati, senza alcun obbligo o formalità.

Art. 11 - Chiavi certificate
La validità di un documento digitale è data dall'apposizione di una chiave asimmetrica di cifratura, generata, assegnata e certificata da uno dei soggetti indicati nel successivo art. 12.
L'autenticazione delle chiavi garantisce pubblicamente l'unicità e l'autenticità delle chiavi stesse, la loro appartenenza al soggetto o ente indicato, il periodo temporale all'interno del quale esse possono essere validamente e legittimamente utilizzate.
La generazione e la trasmissione delle chiavi devono avvenire con le procedure indicate dal regolamento, in modo che la chiave privata non possa venire a conoscenza di soggetti diversi dall'intestatario, anche all'interno dell'ufficio che genera e autentica le chiavi stesse. *(NOTA: questa procedura è normalmente in uso per la generazione dei PIN del Bancomat, e nemmeno l'operatore del sistema può conoscere la chiave privata del titolare della carta).*
Le chiavi private non possono essere archiviate, in qualsiasi forma e a qualsiasi scopo, da soggetti diversi dall'assegnatario.
Nell'ambito della pubblica amministrazione le chiavi sono generate e certificate da appositi uffici da costituirsi all'interno di ogni amministrazione centrale o funzionari abilitati all'interno di enti di particolare rilevanza, secondo i criteri stabiliti dal regolamento di attuazione. Tutte le chiavi pubbliche della pubblica amministrazione devono essere comunicate all'AIPA, presso la quale viene istituito un apposito registro. L'AIPA trasmette le chiavi al registro generale pubblico descritto al successivo art. 13.
Le chiavi da usare nelle trattative private da parte di qualsiasi soggetto possono essere generate, autenticate e comunicate al registro generale pubblico da consorzi di operatori o altre strutture, costituite secondo le direttive emanate dall'Ufficio centrale delle chiavi di cifratura e autenticazione.
Le chiavi per l'autenticazione dei documenti relativi ad atti di straordinaria amministrazione sono generate e autenticate da un notaio, che le comunica all'apposito archivio delle chiavi notarili. Per atti di particolare rilevanza, elencati nel regolamento o indicati dalla sezione notarile dell'Archivio unico delle chiavi di cifratura e codificazione, istituito ai sensi del successivo art. 12, o su richiesta del soggetto interessato, in deroga al divieto indicato dal precedente comma 3, possono essere archiviate anche le chiavi private, generate e certificate espressamente e limitatamente per il documento o il gruppo di documenti relativi al singolo atto.

Art. 12 - Organismi competenti
La generazione e la certificazione delle chiavi di cifratura sono compiute da pubblici ufficiali o da funzionari dello Stato espressamente abilitati, o da enti consortili privati, con i requisiti e le modalità previste nell'emanando regolamento.
Il Governo è delegato per la creazione e regolamentazione dei seguenti organismi, la cui attività si svolgerà nell'ambito e con gli strumenti tecnologici della Rete Unitaria della Pubblica Amministrazione:
1) L'Archivio unico delle chiavi di cifratura e autenticazione, con il compito di gestire il Registro pubblico delle chiavi di cifratura e di coordinare tutte le attività inerenti alla documentazione digitale; nell'ambito dell'archivio sono costituite la sezione per il coordinamento delle chiavi generate e certificate da uffici privati e la sezione per le chiavi di competenza notarile.
2) L'Ufficio centrale delle chiavi di cifratura e autenticazione della pubblica amministrazione, in seno all'Autorità per l'informatica nella pubblica amministrazione, con il compito di generare e certificare le chiavi dei soggetti istituzionali e dei pubblici funzionari abilitati alla generazione e alla cerficazione delle chiavi della pubblica amministrazione e dei privati.

Art. 13 - Archivio unico delle chiavi di cifratura e autenticazione
È costituito l'Archivio unico delle chiavi di cifratura e autenticazione...
Nella sostanza vanno mantenute le previsioni dell'attuale art. 13. L'ufficio gestisce il registro pubblico delle chiavi, consultabile da chiunque gratuitamente e anche per via telematica.

Articoli successivi: rimane la sostanza del progetto dell'AIPA, con le modifiche che derivano dagli articoli precedenti.