di Manlio Cammarata

Arrivano i regolamenti sul documento elettronico

La rivoluzione digitale incomincia adesso

Con l'emanazione dei regolamenti previsti dalla legge del 15 marzo scorso, atti, documenti e contratti pubblici e privati, formati e trasmessi con mezzi elettronici sono "validi e rilevanti a tutti gli effetti di legge". Sarà una rivoluzione o un'altra occasione perduta?

"Il documento digitale, una svolta storica" era il titolo che, solo dieci mesi fa, annunciava su MCmicrocomputer n. 168 il progetto sulla certificazione elettronica presentato dall'Autorità per l'informatica nella pubblica amministrazione. "Un passaggio epocale" lo aveva definito il notaio Enrico Maccarone, uno degli estensori del progetto, nell'intervista che accompagnava l'articolo. Ora siamo alla "rivoluzione digitale": troppo entusiasmo?

Per capirlo dobbiamo riflettere anche sul secondo articolo (MCmicrocomputer n. 169, gennaio '97), pubblicato un mese dopo il primo, che si intitolava "Toppa burocrazia per il documento digitale": si vedevano da una parte le premesse sostanziali per la "svolta storica", dall'altra tutto il peso della cultura burocratica, con i suoi inutili passaggi, le sue gerarchie, che complicavano senza ragione un meccanismo per sua natura molto semplice ed efficace. Ora, con l'emanazione dei regolamenti applicativi della "Bassanini 1", la sovrastruttura sparisce come per incanto e resta solo la sostanza. E siccome sulla formazione e la trasmissione dei documenti si fonda l'intero meccanismo della pubblica amministrazione, tutto l'apparato burocratico viene scosso dalle fondamenta e dovrebbe trasformarsi completamente nel giro di cinque anni, come vedremo tra poco.

Il termine di 180 giorni previsto dalla legge per l'emanazione dei regolamenti scade nella seconda metà di settembre. Mentre scrivo, alla metà di luglio, l'AIPA ha reso noto solo il testo di uno dei quattro regolamenti previsti, il più importante, perché riguarda tutto il sistema della certificazione digitale sia per il sistema pubblico, sia per i rapporti privati; gli altri sono destinati alle specifiche tecniche e alle procedure della pubblica amministrazione e quindi meno significativi per una visione complessiva dell'argomento. Va detto anche che il testo (riportato per intero su InterLex alla URL http://www.interlex.com/testi/attielet.htm) potrebbe subire ancora qualche modifica, ma la sostanza è ormai definita. Deve entrare in vigore 120 giorni dopo la sua pubblicazione: possiamo quindi dire che il futuro è vicinissimo.

Vediamo ora gli aspetti più significativi dell'articolato, che porta il titolo "Schema di Regolamento concernente: Atti, documenti e contratti in forma elettronica". Dispiace rilevare che è stata mantenuta la dizione "elettronica", mentre sarebbe stata più corretta quella di "digitale" o "informatica", perché "elettronici" sono anche una vecchia radio a valvole o un forno a microonde, che non hanno nulla a che fare con la materia di cui ci stiamo occupando.

La fine del medioevo cartaceo

Il punto di partenza, potremmo dire "il manifesto della rivoluzione", è il secondo comma dell'articolo 15 della legge 15 marzo 1997, n. 59 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa". Dice: *Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri di applicazione del presente*

comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare, entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi.. .eccetera eccetera.

Tutto qui. Sembra poca cosa ma in realtà è il segno di un cambiamento sostanziale. Infatti l'articolo 1 della vecchia bozza di disegno di legge dell'AIPA (http://www.aipa.it/notaria/notaria.htm) affermava: *Ogni atto e documento, con qualsiasi procedimento ed a qualsiasi fine emanato o prodotto, contenuto in originale o in copia su uno dei supporti informatici a tecnologia avanzata individuati ai sensi del successivo art. 2, ovvero trasmesso per via telematica ai sensi del successivo art. 4, ed intelligibile mediante l'uso di programmi per elaboratore elettronico, ha l'efficacia probatoria del corrispondente documento cartaceo se è stato redatto con le caratteristiche previste dalla presente legge e dal suo regolamento di attuazione.* La differenza è sostanziale, perché la bozza diceva, in sostanza, che il documento elettronico "ha l'efficacia probatoria del corrispondente documento cartaceo", mentre l'attuale regolamento afferma che esso è di per sé "valido e rilevante a tutti gli effetti di legge". Tralasciamo la disquisizione strettamente giuridica sulla differenza tra "efficacia probatoria" e "validità e rilevanza a tutti gli effetti di legge" (è comunque evidente che la prima espressione è più restrittiva), il punto fondamentale è che nella prima formulazione il documento cartaceo restava come "il vero" documento e quello "contenuto su un supporto a tecnologia avanzata" un sostituto, mentre nella legge 59/97 il documento formato e trasmesso con strumenti informatici è valido in quanto tale, senza nessun riferimento alla forma cartacea. Possiamo definire questo passaggio come una vera e propria rivoluzione culturale.

Per completare il quadro leggiamo altri due punti.

Art. 18. (Documenti informatici delle pubbliche amministrazioni) 1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

Art. 20. (Rete unitaria) 1. Ogni pubblica amministrazione utilizza la rete unitaria di interconnessione telematica per lo scambio di dati, atti e documenti con altre amministrazioni e con i privati anche in conformità alle disposizioni del presente regolamento e secondo le norme tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione. 2. Le pubbliche amministrazioni provvedono, entro cinque anni, a partire dal 1 gennaio 1998, a progettare, a revisionare e a realizzare sistemi informativi finalizzati alla totale automazione delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti in conformità alle disposizioni del presente regolamento.

In sintesi:

a) il documento informatico è informazione "primaria ed originale";

b) la pubblica amministrazione deve usare la rete unitaria per scambiare i documenti, e quindi deve adottare il documento digitale;

c) entro il 1° gennaio 2003 la PA deve passare alla "totale automazione", cioè di fatto potrebbe abolire il documento cartaceo;

d) la PA deve scambiare i documenti in rete anche con i privati, e quindi i privati devono adottare il documento informatico. Un'interpretazione letterale e un po' tendenziosa dell'articolo 20 porta a concludere, per esempio, che anche il 740 e gli altri documenti fiscali dovranno obbligatoriamente essere compilati con strumenti informatici e inviati agli uffici finanziari per via telematica.

Questa è la rivoluzione. O l'utopia.

Elementare, Watson!

Tutta la logica del documento informatico si fonda sui principi della crittografia a chiave pubblica, in particolare sull'algoritmo RSA e sul suo più noto derivato, il PGP (Pretty Good Privacy), che dovrebbe diventare lo standard ufficiale in Italia.

Come tutti ormai dovrebbero sapere, questo tipo di algoritmi è fondato sull'uso di una coppia di chiavi di cifratura, una delle quali viene divulgata, mentre l'altra viene accuratamente tenuta segreta dal suo titolare. Se un documento viene cifrato con la chiave pubblica del destinatario, solo lui può leggerlo, decifrandolo con la sua chiave privata. Invece chiunque può aprire un documento cifrato con la chiave privata del mittente, servendosi della chiave corrispondente pubblica, e verificarne l'autenticità, perché se la procedura non funziona vuol dire che non è stato cifrato da chi dice di esserne l'autore.

Si può anche lasciare il testo del documento in chiaro e cifrare con la chiave privata solo la firma e altre indicazioni, come la data e l'ora del mittente e anche una "impronta" del testo. Se questa parte del documento può essere decifrata con la chiave pubblica dell'autore, si ha la certezza dell'autenticità del testo e di tutte le altre informazioni. Siccome è praticamente impossibile ricostruire la chiave privata partendo da quella pubblica o decrittare il documento con altri sistemi, il metodo è molto sicuro, più sicuro delle firme autografe, dei timbri e dei sigilli tradizionali. Questa è la base del "documento informatico" valido a tutti gli effetti di legge.

Naturalmente è necessario che chiunque possa controllare che una certa chiave pubblica appartenga a un determinato soggetto, e per questo sono importanti le procedure di certificazione e pubblicazione delle chiavi, delle quali parleremo in un prossimo articolo.

Chi vuole saperne di più può rileggere le note di Corrado Giustozzi sul n. 168 di MCmicrocomputer, riportate anche su InterLex alla URL http://www.interlex.com/docdigit/corrado1.htm. E su InterLex daremo conto tempestivamente anche di tutti gli sviluppi della situazione, a partire dai testi degli altri regolamenti a mano a mano che saranno resi pubblici.

Il documento informatico

Naturalmente non tutte le scritture o gli altri elaborati informatici sono "documenti" nel senso previsto della legge. Per esempio, questo articolo, scritto col PC e inviato alla redazione via e-mail non è un documento "valido e rilevante a tutti gli effetti di legge". Ma potrebbe diventarlo se venisse corredato di una "firma digitale", generata e apposta secondo le disposizioni del regolamento. Per capire bene il meccanismo bisogna procedere con ordine e ripartire dai primi tre articoli, che sono riportati negli estratti del testo che trovate in queste pagine. Per inciso, le regole tecniche (og-

Definizioni e principi

In questi riquadri sono riportati i passaggi più importanti del regolamento "Atti, documenti e contratti in forma elettronica". Il testo completo è su InterLex alla URL http://www.interlex.com/testi/attielet.htm

Art. 1. (Definizioni)
1. Ai fini del presente regolamento s'intende:
a) per documento informatico, la rappresentazione informatica di atti o fatti giuridicamente rilevanti;
b) per firma digitale, il risultato della procedura informatica che rende manifesta e consente di verificare la riferibilità soggettiva e l'integrità di un documento informatico o di un insieme di documenti informatici;
c) per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre firme digitali o di verificarne la validità;
d) per chiavi asimmetriche, la coppia inscindibile di chiavi crittografiche da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;
e) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare;
f) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere divulgato;
g) per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica di una coppia di chiavi asimmetriche, rilevabile dai sistemi di validazione, mediante la quale si garantisce la unicità ed univocità della coppia, la sua appartenenza ad un soggetto ed il periodo di loro validità;
h) per chiave biometrica, la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente;
i) per validazione temporale, il risultato della procedura di elaborazione informatica, conforme alle disposizioni del presente regolamento, per attribuire ad uno o più documenti informatici una data ed un orario opponibili ai terzi;
j) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici.

Art. 2. (Documento informatico)
1. Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.

Art. 3. (Requisiti del documento informatico)
1. La formazione, trasmissione, conservazione, duplicazione e riproduzione dei documenti informatici debbono essere conformi alle regole tecniche individuate con decreto del Presidente del Consiglio dei Ministri su parere conforme dell'Autorità per l'informatica nella pubblica amministrazione.

Art. 4. (Forma scritta)
1. Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta.

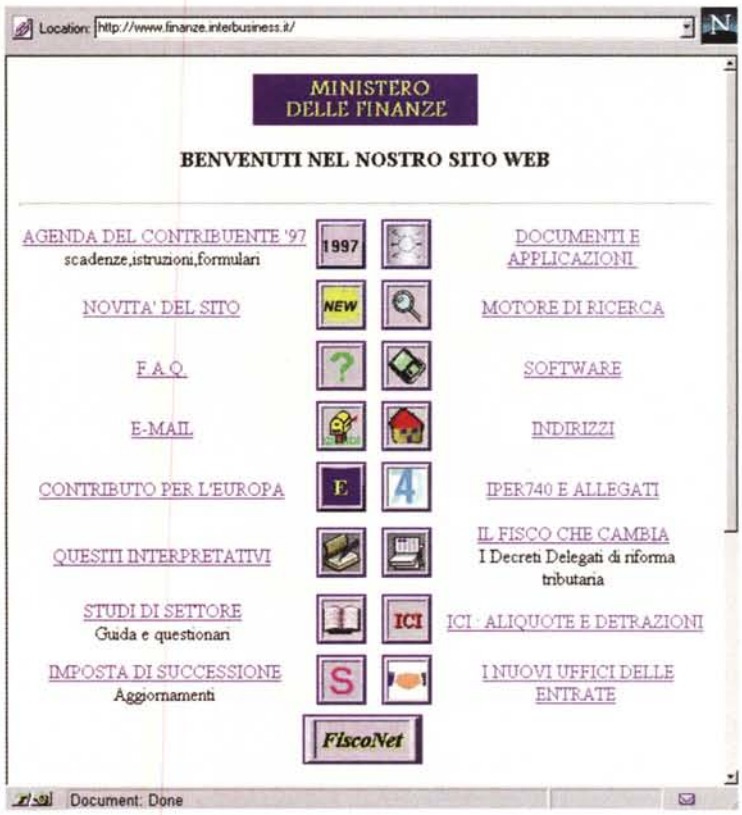
Art. 5. (Efficacia probatoria del documento informatico)
1. Il documento informatico munito dei requisiti previsti dal prsente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2714 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

Art. 6. (Copie di atti e documenti)
1. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.
2. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia probatoria, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente regolamento.
3. 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.
4. La spedizione o il rilascio di copie di atti e documenti di cui al comma 2 esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richiesta ad ogni effetto di legge.
5. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 3.

Art. 7. (Deposito della chiave privata)
1. Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata con le modalità e nelle forme di cui all'art. 605 del codice civile.

Art. 8. (Adempimenti preliminari)
1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.
2. Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del soggetto, pubblico o privato, che le ha certificate e, dal momento iniziale della loro validità, sono consultabili in forma telematica.

Art. 9. (Responsabilità civile)
1. Chiunque cagiona danno ad altri per effetto dell'uso di un sistema di chiavi asimmetriche o della firma digitale, è tenuto al risarcimento se non prova di aver adottato tutte le misure idonee ad evitare il danno.



Il sito del Ministero delle Finanze (http://www.finanze.interbusiness.it/) è un esempio di come la pubblica amministrazione potrebbe comunicare con i cittadini in un futuro abbastanza vicino.

getto di un altro regolamento) dovrebbero essere in sostanza quelle relative all'uso del protocollo PGP, largamente diffuse sul Web e facilmente reperibili a partire dal sito di PGP International (http://www.ifi.uio.no/pgp).

Il testo dei primi tre articoli è abbastanza chiaro e non richiede particolari spiegazioni o commenti. Il quarto, il quinto e il sesto sono importantissimi, perché sanciscono che il documento informatico soddisfa la "forma scritta" ogni volta che essa è prevista dalle disposizioni vigenti: non c'è nessuna differenza, in nessun caso, tra documento cartaceo e documento digitale.

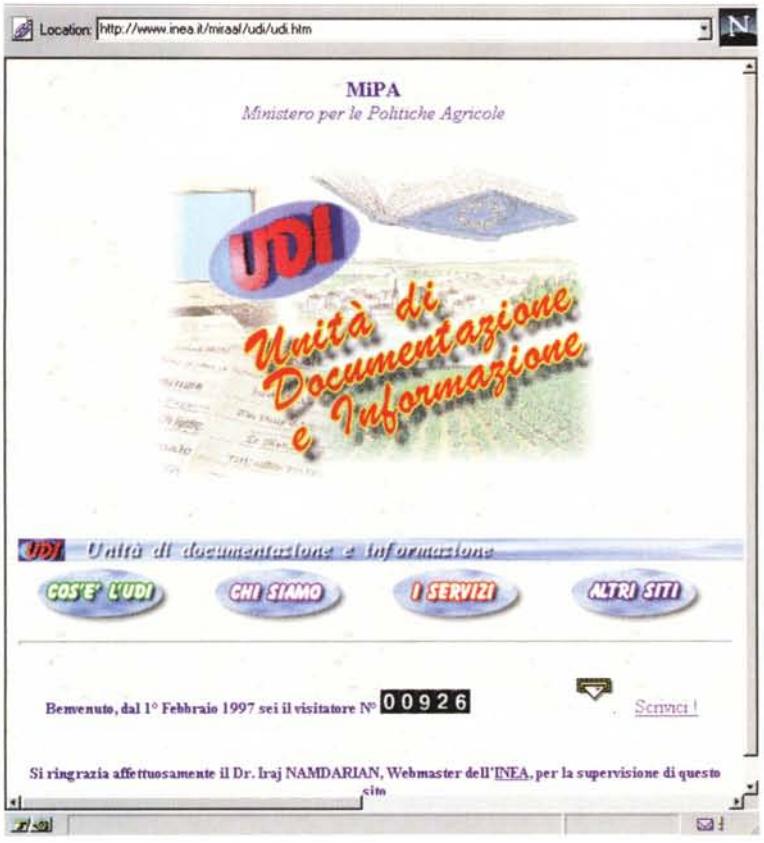
L'ordine logico dei successivi due articoli appare invertito: l'ottavo prescrive che chiunque intenda usare un sistema di cifratura a chiavi asimmetriche deve sottoporre a certificazione la chiave pubblica, mentre nel settimo si dice che il titolare può ottenere il deposito della chiave privata con le stesse rigorose formalità del "testamento segreto": *la carta [...] che serve da involto deve essere sigillata con una impronta, in guisa che il testamento non si possa aprire né estrarre senza rottura né alterazione. Il testatore, in presenza di due testimoni, consegna personalmente al notaio la carta sigillata, o la fa sigillare nel modo sopraindicato in presenza del notaio e dei testimoni, e dichiara...* Tralasciamo i successivi dettagli del cerimoniale, ma teniamo a mente questo articolo, perché tra poco ne capiremo l'importanza.

L'articolo 9 disciplina la responsabilità civile per i danni che possono essere causati con l'uso di un sistema di cifratura: c'è la cosiddetta "inversione dell'onere della prova", per la quale non è il danneggiato che deve provare il nesso di causalità tra l'azione e il danno, ma è il convenuto che deve provare di aver preso tutte le misure idonee a evitarlo. La disposizione è comprensibile se si riflette sull'estrema importanza della "firma digitale" e della delicatezza di molti atti per i quali può essere impiegata. La stessa disposizione vale per il depositario della chiave pubblica che ometta o ritardi la pubblicazione della revoca o della sospensione della chiave.

La firma digitale

Con l'articolo 10 si apre il capo II, dedicato alla "firma digitale", che è il requisito fondamentale del documento informatico. E' bene ricordare che gli algoritmi di cifratura a chiave pubblica (si vedano le note di Corrado Giustozzi su MCmicrocomputer n. 168) servono a due funzioni diverse: la cifratura delle informazioni, cioè la procedura che rende un documento leggibile solo dal destinatario, e anche l'autenticazione del contenuto, dell'identità del mittente ed eventualmente della data e dell'ora della formazione o della spedizione.

Secondo le prescrizioni di questo articolo, la firma digitale (che deve avere particolari caratteristiche) equivale alla firma tradizionale e sostituisce punzoni, sigilli, timbri e ogni altro sistema di validazione. E' importante il comma 8, che prescrive l'indicazione del soggetto che ha certificato la chiave e del registro pubblico nel quale può essere controllata. Questo è un punto essenziale, perché la validità di una firma è subordinata alla sua verificabilità; quindi è necessario che la chiave pubblica attraverso la quale è stata generata sia controllabile da chiunque. Per questo serve la procedura prevista dal già citato articolo 8: chi vuole servirsi della firma digitale deve depositare la chiave pubblica in un registro consultabile da chiunque, anche per via telematica, e questa è la "certificazione". In pratica, se ricevo un documento provvisto di firma digitale, devo controllare che la chiave pubblica indicata dal mittente corrisponda effettivamente a quella pubblicata e quindi certificata. Se, applicando questa chiave alla firma digitale, si rendono chiare le indicazioni che contiene, vuol dire che essa è stata generata proprio con la chiave privata di chi afferma di essere il mittente.



Il sito del Ministero per le Politiche Agricole, ovvero come fare la fila anche sul Web, nell'attesa che si formi la grande e inutile immagine (http://www.inea.it/miraaf/udi/udi.htm)...

Con la stessa procedura si verifica se il contenuto del documento non sia stato alterato e, con un'ulteriore verifica della chiave di un organismo certificatore, posso essere certo anche della data e dell'ora in cui è stato formato o spedito. Se c'è stata una qualsiasi alterazione la procedura non funziona, quindi l'avvenuta decifrazione fornisce la certezza dell'autenticità di tutte le informazioni contenute nel documento.

Gli articoli 11 e 12 estendono al settore privato la validità del documento informatico. Sono norme importanti per lo sviluppo annunciato del commercio telematico e di tutte le transazioni private e rendono possibile lo scambio on-line di qualsiasi informazione di rilevanza giuridica. Ma è l'articolo 13 quello sul quale bisogna soffermarsi con più attenzione. Dice infatti il comma 1 che *La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione telematica sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria.*

A prima vista si tratta semplicemente dell'estensione (forse non strettamente necessaria) dell'articolo 15 della Costituzione alla corrispondenza digitale, ma in realtà ha un valore molto più alto, perché elimina qualsiasi discussione sul "key escrow" (l'affidamento a un'autorità della chiave privata, che consentirebbe di "aprire" la corrispondenza telematica in caso di indagini penali). Questa previsione era contenuta nel primo documento dell'AIPA e aveva suscitato molte critiche (si veda ancora il n. 168 di MCmicrocomputer, il testo è anche su InterLex alla URL http://www.interlex.com/docdigit/mc168.htm). Purtroppo molti governi non si rendono conto della sostanziale inutilità del key escrow a fini di giustizia e dei rischi che esso comporta per la libertà individuale. Il primo comma dell'articolo 13 è un segno di alta civiltà giuridica, oltre che di elementare buon senso, e consente di apprezzare la procedura di deposito della chiave privata prevista dall'articolo 7, con il suo rigido cerimoniale: la comunicazione della chiave privata a un altro soggetto, sia pure a un pubblico ufficiale come il notaio, va compiuta con particolari formalità perché costituisce un atto assolutamente straordinario.

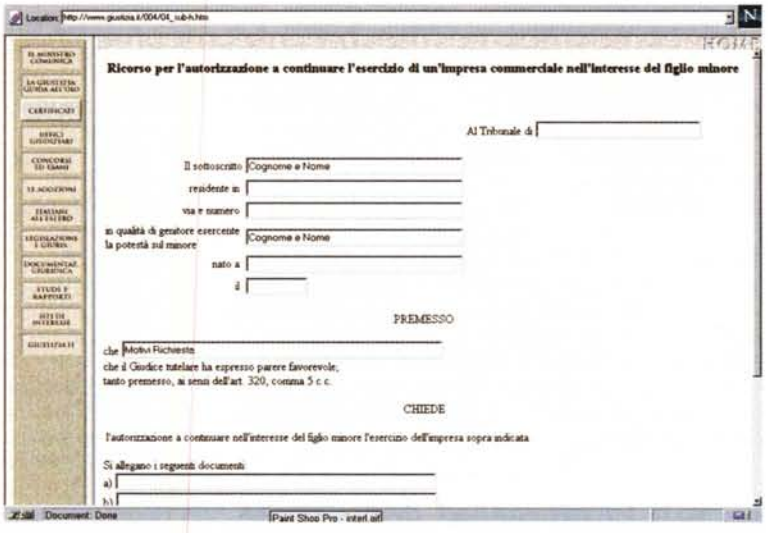
Il notaio on-line

Visto che siamo in tema di atti straordinari, passiamo all'articolo. 16, che tratta della firma digitale autenticata (il 14 e il 15 si occupano dei pagamenti informatici e dei libri e delle scritture di cui sia obbligatoria la tenuta; ce ne occuperemo quando sarà possibile esaminare le norme tecniche). Che cosa è la firma digitale autenticata, che si aggiunge a quella certificata a norma dell'articolo 8? La legge prescrive che per alcuni atti, detti "di straordinaria amministrazione", come la compravendita di immobili, la semplice firma non basta. Occorre che un pubblico ufficiale (notaio, segretario comunale o un altro soggetto autorizzato) certifichi che la firma è stata apposta in sua presenza, dopo essersi accertato dell'identità del soggetto e di altri requisiti del soggetto stesso e dell'atto che viene sottoscritto. L'articolo 16 estende queste disposizioni al documento digitale, sottolineando che il pubblico ufficiale deve accertarsi che la chiave utilizzata sia valida e che il documento non deve essere in contrasto con l'ordinamento giuridico.

Riassumendo, chiunque può avere una chiave certificata, che serve per tutti i documenti e gli atti di ordinaria amministrazione, mentre per ciascun atto di straordinaria amministrazione, dove la legge prescrive la firma autenticata, occorre appunto la firma digitale autenticata. Il regolamento non dice espressamente, ma il senso è chiaro dal combinato disposto delle norme precedenti, che anche l'autenticazione può avvenire in forma digitale. E' sempre necessaria la presenza fisica del-

l'interessato di fronte al pubblico ufficiale, ma quest'ultimo può apporre la sua firma digitale all'atto di autenticazione digitale.

Passiamo all'articolo 17, dove si dice che ogni pubblica amministrazione provvede autonomamente alla generazione, alla conservazione, alla pubblicazione e all'utilizzo delle chiavi di propria competenza. Un altro colpo d'ariete alla cultura burocratica: la prima bozza prevedeva tutta una serie di autorità per questo specifico compito, ora prevale la "logica della rete". Perché, se il fondamento di tutto il meccanismo è la verificabilità della chiave pubblica da parte di chiunque, basta un elenco consultabile su Internet, senza formalità particolari o inutili gerarchie.



Ministero di Grazia e Giustizia: i moduli online, uno sguardo al futuro. Si possono compilare a video ma, per ora, vanno stampati su carta (http://www.giustizia.it/004/04_sub-h.htm).

Ma nulla è perfetto, e il secondo comma di questo articolo presenta uno dei più allucinanti capolavori dell'italica crittografia legislativa. Si tratta di una specie di scioglilingua: *Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente, nell'ambito delle leggi e dei regolamenti che definiscono l'uso delle firme analogiche nell'ambito dei rispettivi ordinamenti giuridici.* E chi saranno mai "i pubblici ufficiali non appartenenti alla pubblica amministrazione"? I notai, proprio i notai, con i loro mantelli a ruota! Sembra di capire che la pubblicazione delle loro chiavi debba seguire le stesse procedure previste per la firma autografa e il prezioso "sigillo", ma evidentemente ci sarà qualche differenza, perché non c'è una coppia di sigilli, pubblico e privato...

Scherzi a parte, l'istituzione del "notaio informatico" è un fatto di grande importanza, perché è un vero colpo al cuore del principio cartaceo che co-

Firma digitale, corrispondenza, contratti

Art. 10. (Firma digitale)
1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta o associata una firma digitale.
2. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.
7. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.
8. Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti con il decreto di cui all'articolo 3, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

Art. 11. (Contratti stipulati con strumenti informatici o per via telematica)
1. I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge.

Art. 12. (Trasmissione del documento)
1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.
2. La data e l'ora di redazione, di spedizione o di ricezione di un documento informatico redatto in conformità alle disposizioni del presente regolamento sono opponibili ai terzi.
3. La trasmissione del documento informatico per via telematica equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Art. 13. (Segretezza della corrispondenza trasmessa per via telematica)
1. La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione telematica sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria.

Art. 14. (Pagamenti informatici)
1. Il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art. 15. (Libri e scritture)
1. I libri, i repertori e le scritture, di cui sia obbligatoria la tenuta sono, di norma, formati e conservati su supporti informatici in conformità alle disposizioni del presente regolamento e secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art.16. (Firma digitale autenticata)
1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.
3. L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

stituisce il fondamento dei sistemi "di diritto latino". Per inciso, il "cybernotaio" è stato recentemente istituito in Florida, ma con implicazioni in qualche misura diverse a causa dei principi della *Common Law*: ne parleremo sul prossimo numero, perché potrebbe essere un passaggio importante verso un "diritto del meta-territorio Internet" comune a paesi con ordinamenti giuridici assai differenti. All'istituzione del "sigillo elettronico" corrisponde un'evoluzione di tutta l'attività notarile, con la possibilità di stipulare atti tra soggetti che si trovano in luoghi diversi e di trasmettere documenti alla pubblica amministrazione per via telematica. Si aggiunga che anche il settore degli studi legali è alla vigilia di innovazioni di questo tipo, con la progressiva istituzione dei siti Web delle sedi giudiziarie; le sperimentazioni stanno per partire.

La pubblica amministrazione e la rete

Dell'articolo 18 e dei seguenti, che riguardano in particolare la pubblica amministrazione, abbiamo già parlato all'inizio dell'articolo. Il documento informatico non è solo il requisito essenziale per il funzionamento della rete unitaria, ma anche lo strumento per applicare - finalmente - le previsioni della legge 241/90 sulla trasparenza amministrativa e assicurare ai cittadini il diritto di accesso ai documenti.

L'aspetto più significativo è costituito dal cambiamento del principio stesso della certificazione: nel sistema cartaceo gli effetti legali di un documento sono legati all'autenticazione del supporto che lo contiene; se le informazioni sono trasferite su un altro supporto occorre una nuova autenticazione. E' superato anche il tentativo di autenticazione "alla fonte" contenuto nel decreto legislativo 39/93, istitutivo dell'AIPA (norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche). Ora l'autenticazione è "incorporata" nel documento e può seguirlo in tutti i suoi passaggi, senza alcun riferimento al supporto.

Gli effetti sono facilmente immaginabili: i cittadini smetteranno di fare i portalettere per conto degli uffici pubblici e persino i tanto celebrati "sportelli polifunzionali" - che di fatto si stanno rivelando molto meno efficaci del previsto, anche perché ancora poco diffusi - non avranno più ragione di esistere, dal momento che ogni PC collegato a Internet sarà uno sportello polifunzionale per le operazioni alle quali sarà abilitato il suo possessore o il suo addetto.

Se combiniamo le previsioni del progetto della rete unitaria della pubblica amministrazione con le norme sul documento informatico otteniamo il disegno di un sistema *client-server* che ricalca perfettamente il "modello Internet". Questa tendenza è ancora più evidente se consideriamo il salto che è stato fatto (in pochi mesi) dal primo progetto al testo attuale. E' scomparso, completamente scomparso, tutto l'apparato burocratico previsto all'inizio. Il testo delle regole tecniche rivelerà il segreto di questa incredibile evoluzione: l'adozione delle stesse procedure in uso su Internet, un sistema di enorme estensione e complessità che funziona nell'assenza del concetto stesso di burocrazia.

A questo punto però si ripresenta il dubbio espresso all'inizio: rivoluzione o utopia?

L'esperienza, purtroppo, favorisce la seconda ipotesi. Siamo amministrati da un sistema che in quasi trent'anni è riuscito a non

La pubblica amministrazione

Art. 18. (Documenti informatici delle pubbliche amministrazioni)
1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

Art. 19. (Sottoscrizione dei documenti informatici delle pubbliche amministrazioni)
1. In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa, o la sottoscrizione comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente regolamento.

Art. 20. (Rete unitaria)
1. Ogni pubblica amministrazione utilizza la rete unitaria di interconnessione telematica per lo scambio di dati, atti e documenti con altre amministrazioni e con i privati anche in conformità alle disposizioni del presente regolamento e secondo le norme tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione.
2. Le pubbliche amministrazioni provvedono, entro cinque anni, a partire dal 1 gennaio 1998, a progettare, a revisionare e a realizzare sistemi informativi finalizzati alla totale automazione delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti in conformità alle disposizioni del presente regolamento.
5. Entro il 31 dicembre 1998, le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia opportuna od obbligatoria la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici.

Art. 22. (Formulari, moduli e questionari)
1. Entro il 31 dicembre 1998 le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge per l'interscambio dei dati nell'ambito della rete unitaria e con i soggetti privati.

EPSON Stylus Photo e FilmScan 200. E' nata la camera oscura digitale.

Da oggi chi è appassionato di fotografia ha veramente strumenti dedicati: EPSON FilmScan 200 è uno scanner per acquisire automaticamente diapositive e negative 35 mm alla risoluzione ideale (ben 1200x2400 dpi) per elaborarle, archiviarle (c'è anche in dotazione il software necessario, sia per Windows che per Mac) o stamparle.

E poi c'è EPSON Stylus Photo, la ink jet appositamente creata per stampare fotografie ad alta risoluzione (720x720 dpi con Super MicroDot) e con tutta la morbidezza delle sfumature data dalla stampa in esacromia, dai nuovi inchiostri Quick-Dry e da AcuPhoto Halftoning, che oltre a migliorare ulteriormente le sfumature aiuta ad ottenere una migliore corrispondenza tra i colori a monitor e quelli di stampa.

Oltre che con i driver per Windows e per Macintosh, EPSON Stylus Photo viene venduta con LivePix, un software di trattamento e archiviazione delle immagini completo di una libreria di schemi grafici per realizzare facilmente cartoline, biglietti, calendari e perfino magliette personalizzate.

Vorrei saperne di più ❑ su EPSON FilmScan 200
❑ su Stylus Photo, e ricevere una prova di stampa.

Nome_____

❑ casa ❑ ufficio Società_____

Indirizzo_____

CAP_____ Città_____

❑ per non ricevere ulteriori comunicazioni, barrare la casella.

MC MICROCOMPUTER

Spedire a: EPSON Italia SpA - 20099 Sesto S. Giovanni (MI) V.le F.lli Casiraghi 427, o inviare via fax allo 02/2440750.

Per informazioni sui punti vendita, chiamare il Numero Verde **167-801101**

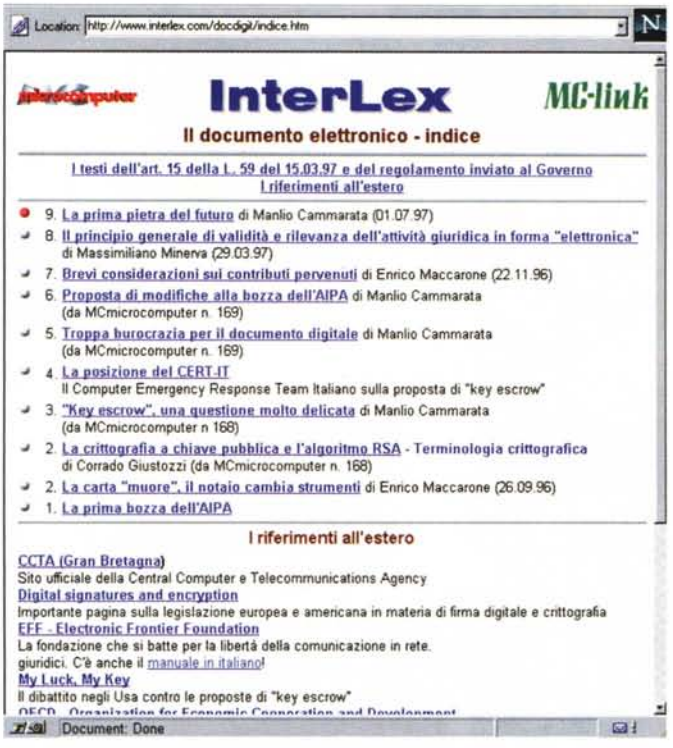
In Internet: www.epson.it

Vieni a trovarci allo SMAU Pad. 11 Stand F16/H09

ImmaginEmozione

EPSON®

Si possono seguire su InterLex le novità e il dibattito sul documento digitale (http://www.interlex.com).



applicare la legge sull'autocertificazione e che da sette anni cerca in tutti modi di sfuggire alle regole sulla trasparenza della pubblica amministrazione. Un paese dove i notai sono indicati come "pubblici ufficiali non appartenenti alla pubblica amministrazione" e dove la legge sulla protezione della riservatezza non si applica a una certa banca di dati personali, anzi no, non si applica ad eccezione di certi articoli, ma con l'eccezione di certi altri, e se non hai la possibilità di consultare l'archivio delle leggi non sai che la banca in questione è proprio quella delle forze di polizia, la più misteriosa e la più pericolosa. Ma non hai la possibilità di consultare l'archivio delle leggi, perché non solo è criptico il loro testo, ma anche l'accesso all'archivio è difficile, protetto da formule esoteriche che richiedono una lunga e difficile iniziazione e dal pagamento di un obolo esorbitante. E i custodi ti dicono anche sarebbe inutile renderti più facile l'accesso alla legge perché tu, cittadino ignorante, non saresti comunque in grado di capirla. Un paese dove la pubblica amministrazione apre i suoi siti Internet, ma solo per indicarti i luoghi dove andare a fare la fila per chiedere i documenti; dove le università si mettono "on-line" con l'unico scopo di pubblicare gli elenchi delle facoltà e i nomi degli accademici - dei quali, a differenza degli analoghi siti di altri paesi, non rivelano il numero di telefono né l'ipotetico indirizzo e-mail - dove si inventano gli URP (Uffici per le Relazioni con il Pubblico) per frapporre altra burocrazia tra il cittadino e l'esercizio dei suoi diritti. Per capire bene quale distanza separi la politica e la burocrazia italiana da una visione democratica del rapporto col cittadino, riprendiamo la legge 241/90, dove si dice che *Al fine di assicurare la trasparenza dell'attività amministrativa e di favorirne lo svolgimento imparziale, è riconosciuto a chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti il diritto di accesso ai documenti amministrativi, secondo le modalità stabilite dalla presente legge* (art. 22, comma 1). Ora facciamo un salto oltre oceano e diamo un'occhiata al "Freedom of Information Act", la legge degli Stati Uniti che dal 1977 regola l'accesso dei cittadini ai documenti amministrativi. Inizia così: *Ogni amministrazione deve rendere disponibili le informazioni al pubblico...* (il testo del FOIA, con una guida per il cittadino - americano - e tutti i riferimenti utili si trova alla URL http://www.comedia.com/ftp/think/freedom/foia.guide). Questa è la differenza: qui il "suddito" deve prima dimostrare che ha un legittimo interesse all'accesso ai documenti, là si dice che gli uffici devono mettere i documenti a disposizione dei cittadini. La differenza è sostanziale.

E' vero che recenti leggi cercano di migliorare il funzionamento della pubblica amministrazione e preparano il terreno per innovazioni fondamentali come il documento informatico e la rete unitaria, ma ci vorrà molto tempo prima che si possa cambiare la cultura della burocrazia e demolire le sue ormai secolari stratificazioni di "prassi" e di regolamenti, che hanno generato e consolidato la visione dell'azione amministrativa come finalizzata al corretto svolgimento della procedura e non al risultato di essa. Come saranno accolte dai burocrati le novità dei regolamenti sul documento digitale? Se consideriamo i risultati ottenuti dalla legge 241/90 non possiamo che essere pessimisti. Forse si dovrà aspettare una nuova generazione di funzionari pubblici, ma non sembra che essa si stia formando. Le facoltà di giurisprudenza, dalle quali esce la maggior parte dei burocrati, sono ancora pervase dalla cultura della carta. Non si insegna, se non in pochissimi casi, il diritto delle tecnologie; in qualche ateneo ci si trastulla con la cosiddetta informatica giuridica, che di informatico non ha quasi nulla. Comunque tra poco più di un anno potremo trarre qualche indicazione sul modo in cui la pubblica amministrazione accoglierà le norme sul documento informatico: basterà contare quanti uffici avranno applicato l'articolo 22 del regolamento: *Entro il 31 dicembre 1998 le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge per l'interscambio dei dati nell'ambito della rete unitaria e con i soggetti privati.*
Questo significa che nei prossimi mesi tutte le pubbliche amministrazioni dovranno avere un sito Web efficiente. O no?

Chi trova un amico... non spende un tesoro

Hans ha detto a Yamen che quando Thomas parla con Ingrid o

Paula deve fissare con Keiko per chiedere a Yutta di domandare a Bob se

Pablo può richiamare Anna per sentire Chen se quando Ingmar...

MMX™ intel inside pentium® PROCESSOR

Leonhard & Galileo

• M/B ASUS TX97-E 512Kb • Processore Intel Pentium® con tecnologia MMX™ 200 MHz • Ram 32 Mb EDO • HDD 3,2 Gb EIDE • CD ROM 24X CDR-8330 HITACHI • Matrox Mistique 220 4Mb + giochi • Matrox Rainbow Runner • Fax-Modem33600 DIGICOM • Tastiera 105 tasti Win'95 NMB • Sound Blaster 16 PnP • Speakers 60W • Mouse seriale • WINDOWS '95, Media studio, iPhoto Express, VDOphone, MPEG1 • VIDEOCAMERA digitale colore GALILEO.

Omaggio:
abbonamento 2 mesi Internet

L. 3.099.000

Videoincontriamoci con Frael

Un sorriso ispira simpatia e mette di buon umore. Frael ha deciso di mostrare ai suoi utenti tutti i sorrisi del mondo, per questo propone Leonhard&Galileo: computer dotato di processore Intel Pentium® con tecnologia MMX™ 200 MHz e videocamera digitale a colori. Puoi usarlo per videoconferenze o per conoscere e vedere nuovi amici in tutto il mondo, al costo di una telefonata urbana. Perché con Frael chi trova un amico...non spende un tesoro!

Siamo presenti a **SMAU '97 pad 11 Stand B21.**

Per catalogo e informazioni:
www.frael.it

FRAEL
ELABORATORI ELETTRONICI ITALIANI

**FRAEL Via del Roseto, 50 Vallina • 5001
Bagno a Ripoli (FI) Tel. 055 - 69647
(8linee r.a.) • Fax 055 - 696289 Hot Lir
Divisione Tecnica 055-69631**