Le misure di sicurezza minime per il trattamento dei dati personali

di Nicola Bortolotti

Non ha avuto il medesimo risalto del "giro di vite" su casco e cinture di sicurezza. E probabilmente la sua entrata in vigore rimarrà silente, secondo il costume italiano, sino alla prima (e forse clamorosa) sentenza che inizierà a produrre quel bagaglio di "precedenti" senza i quali leggi ambigue e mal formulate rimangono così criptiche da risultare quasi inapplicabili.

È l'ennesimo corollario della legge 675/96, la cosiddetta "legge sulla *privacy*", che dopo le grottesche dichiarazioni a cui costringe, per limitarsi a casi eclatanti, in ambito Inps e bancario ("se risponde 'no' la sua pratica non potrà essere liquidata", si può ad esempio leggere in molte avvertenze...) è approdata ora al mondo informatico, con implicazioni su società ed enti privati e pubblici non solo civili (con l'obbligo del risarcimento del danno cagionato per effetto del trattamento dei dati personali ai sensi dell'articolo 2050 del codice civile ma anche penali (sino a due anni di reclusione).

Recita infatti l'articolo 36 della legge 675/96:

"Omessa adozione di misure necessarie alla sicurezza dei dati

1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni.

2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino a un anno."

L'articolo 15 della stessa legge così recita:

"Sicurezza dei dati

1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), *della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'autorità per l'informatica nella pubblica amministrazione e il Garante.*

3. Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.

4. Le misure di sicurezza relative ai dati trattati dagli organismi di cui all'articolo 4, comma 1, lettera b), *sono stabilite con decreto del Presidente del Consiglio dei Ministri con l'osservanza delle norme che regolano la materia."*

Il regolamento citato ha visto la luce nello scorso anno (DPR 318/99), è entrato in vigore a fine settembre 1999 ed è dunque pienamente a regime dal 29 marzo 2000 (come rimarcato dal Garante per la protezione dei dati personali tutte le pubbliche amministrazioni, nessuna esclusa, e i soggetti privati che nell'ambito della propria attività pongano in essere trattamenti di dati personali devono adottare le misure minime di sicurezza emanate dal governo con il regolamento n. 318/99. Si viene tuttavia esentati dal presentare ulteriore modello di notifica).

In esso viene fatta una distinzione tra tre diverse tipologie di *computer*: *elaboratori non accessibili da altri elaboratori o terminali* (ossia PC "stand-alone", sezione I); *elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico* (ossia PC connessi tramite una "rete locale" o LAN, sezione II, art. 3, lettera *a)*); infine *elaboratori accessibili mediante reti di telecomunicazioni disponibili al pubblico* (ossia PC in "rete geografica" o WAN, sezione II, art. 3, lettera *b)*).

Sin da questa ripartizione, tuttavia, iniziano i problemi. La puntualizzazione tra parentesi, infatti, non fa parte del testo del DPR e, sebbene tecnicamente fondata e dettata da una logica stringente, può a rigore non essere corretta. Da questa incertezza discende una potenziale e fortissima discrezionalità nell'applicazione della legge.

Un PC apparentemente e normalmente inaccessibile, infatti, può essere temporaneamente "disponibile al pubblico" e oggetto di attacchi, anche seri, al proprio sistema di sicurezza.

Facciamo un esempio concreto. Si pensi ad un *computer* che non sia nemmeno connesso ad una rete locale (fatto raro, peraltro), contenga dati personali e venga saltuariamente utilizzato per navigare su Internet mediante un modem. Come considerare questo PC ai sensi del DPR 318/99?

La logica porterebbe dritti alla sezione I ma, in realtà, questo PC – seppure per periodi di tempo limitato – fa parte addirittura della categoria di cui all'art. 3, lettera *b)*.

Facendo riferimento ai diffusissimi Windows 95/98, un semplice "binding" come quello riportato in figura 1 (se attivato assieme alla condivisione dei *files*) può infatti rendere un PC facile preda anche a distanza di migliaia di chilometri, in modo pressoché invisibile all'utente. Si potrà obiettare che, proprio il sistema operativo di Microsoft, ricorda con un'apposita finestra l'attivazione di questo legame ma questo non basta: esistono molti programmi di "backdoor" (ad esempio il celebre Back Orifice) in grado di installarsi silenziosamente sul proprio PC apparentemente stand-alone e di farlo divenire facile preda su Internet. Siffatti *software* "maliziosi" hanno dimostrato di poter funzionare anche su sistemi operativi maggiormente curati sotto il profilo della sicurezza come, ad esempio, Windows NT.

Il quadro può sembrare iperallarmistico ed in effetti, qualora si adottino le necessarie precauzioni, la situazione può essere tenuta ampiamente sotto controllo.

Ma, per il solo fatto di parlare di "precauzioni necessarie", è evidente il fatto che a un PC, se collegato anche solo saltuariamente a Internet (si veda la figura 2), non siano applicabili – a rigore – le sole raccomandazioni di cui alla sezione I del DPR 318/99 ma si ricada, invece, negli assai più restrittivi obblighi della lettera *b)*, apparentemente dedicata solo ai "provider Internet" e altri soggetti evoluti, e che prevedono addirittura la predisposizione di un "documento programmatico sulla sicurezza" (art. 6).

Premesso il sussistere di un'ampia discrezionalità interpretativa, vediamo comunque nel dettaglio la legislazione in materia premettendo alcuni chiarimenti sulle definizioni ivi utilizzate. Dalla legge 675/96, art. 2:

"Banca di dati" è *qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento*;

"Trattamento" è *qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati*;
"Dato personale" è *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione*;
"Titolare" è *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza*;
"Responsabile" è *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*;
"Diffusione" significa *il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*;
Dall'art. 22 della stessa legge:
"Dati sensibili" sono *i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*;
Dall'art. 1 del DPR 318/99:
"Misure minime" sono *il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 15, comma 1, della legge*;
"Strumenti" sono *i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento*;
"Amministratori di sistema" sono *i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione*.
Si noti che l'amministratore non è identificabile con il titolare del trattamento, poiché quest'ultimo è l'azienda o la p.a. nel suo complesso. Non è tuttavia nemmeno identificabile con il responsabile del trattamento. Si tratta in genere di due figure professionali assai diverse: il "responsabile" è tipicamente un amministrativo mentre l'"amministratore" un tecnico, un sistemista.
Chiarite le definizioni, nel caso di elaboratori stand-alone (con tutte le riserve illustrate in precedenza), se il trattamento dei dati non è effettuato per scopi esclusivamente personali, si dovrà avere cura (art. 2) di: prevedere una parola chiave di accesso ai dati (*password*) e comunicarla agli addetti; ove possibile consentirne la sostituzione in autonomia; individuare per iscritto i soggetti preposti alla custodia delle password o che possono accedere ad informazioni ad esse concernenti.
Tale articolo è facilmente attaccabile, specie dopo anni ed anni in cui in altre leggi, DPCM e in documenti dell'AIPA (Autorità per l'informatica nella pubblica amministrazione) si parla di *smart card*, *smart key* e chiavi biometriche: nel momento in cui è possibile con costi davvero esigui regolare l'accesso al singolo PC mediante smart card o impronta digitale o impronta retinica, stride il richiamo ad una gestione delle *password* stile mainframe. E non c'è neppure un accenno alla politica da seguire nella gestione delle *password*: durata, blacklist, inibizione delle *blank password*...
Venendo ai PC collegati in LAN (rete locale) ma non accessibili dall'esterno (viene dunque escluso qualsiasi gateway ad esempio verso Internet, anche se tramite *proxy* o *firewall*), si dovrà anche (art. 4): attribuire univocamente a ciascun utente o incaricato un codice identificativo; prevedere la possibilità di disattivarlo in caso di perdita dei "privilegi" di accesso o di inattività per oltre sei mesi (lo tengano presente le donne in maternità); proteggere gli elaboratori contro il rischio di intrusione ad opera di programmi *di cui all'articolo 615*-quinquies *del codice penale* (aventi per scopo o per effetto il danneggiamento del sistema informatico), *mediante idonei programmi* ("antivirus"), *la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale*. Sulle "specifiche" richieste agli "antivirus" si potrebbe scrivere molto: qui si ipotizza implicitamente che di questi programmi ne esistano alcuni "ideali", mentre l'inquietante realtà (nota a qualsiasi "amministratore" degno della sua qualifica) è che non esistono antivirus né perfetti né certificati né certificabili né pienamente verificabili, ed il limitarsi ad imporre una "verifica" ogni sei mesi è del tutto privo di significato: si può trattare – a seconda dei casi – di un lasso di tempo eccessivamente lungo o viceversa assai breve. Norme formulate in questo modo non fanno altro che lasciare totale discrezionalità al giudice di turno.
Se i dati oggetto del trattamento sono "sensibili" e/o giudiziari l'accesso sarà regolato da autorizzazioni controllate annualmente, con verifica preventiva. I supporti di memorizzazione potranno essere riutilizzati solo in caso di cancellazione sicura dei dati precedenti (*wiping*); in caso contrario dovranno essere distrutti. Sarà inibito l'accesso ad una stessa applicazione con lo stesso codice identificativo da diverse postazioni di lavoro.
Nel caso di elaboratori accessibili mediante rete di telecomunicazione disponibile al pubblico, nel caso di trattamento di dati sensibili e/o giudiziari dovrà infine essere (art. 6) *predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi: i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi; i criteri e le procedure per assicurare l'integrità dei dati; i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica; l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni. L'efficacia delle misure di sicurezza adottate dev'essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.*
Sulle misure da adottare per strumenti cartacei e non informatici non ci si soffermerà in questa sede.
Interessante la sezione III del DPR 318/99 da cui si evince che *il trattamento per fini esclusivamente personali dei dati* sensibili e giudiziari *effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati*; un'indicazione che segue, del resto, il comma 1 dell'art. 3 della L. 675/96: *Trattamento di dati per fini esclusivamente personali – Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della presente legge, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione.*
In questi casi è dunque sufficiente proteggere la macchina attivando – ad esempio – la *password* all'accensione prevista da ogni Bios? Parrebbe di sì, ma anche in questo caso la formulazione della legge impone attenzione: come acutamente fatto rilevare da Gianni Buonomo nella relazione presentata al Convegno "Misure minime di sicurezza per la protezione dei dati personali" tenutosi a Roma il 22 ottobre 1999

e integralmente consultabile sul prezioso sito/testata www.interlex.com, "l'art. 18 della legge 675/96 prevede che *chiunque cagiona un danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*. Ciò significa che la legge presume la colpa del gestore della banca di dati e – invertendo l'onere della prova – pone a suo carico ogni possibile conseguenza dei danni cagionati a terzi, se egli non prova di avere adottato tutte le misure idonee ad evitare il danno".

E l'articolo 2050 si applica in ogni caso, anche nel caso di banche dati per fini esclusivamente personali (art. 3, comma 2, L. 675/96).

Non è facile trovare su Internet esattamente le informazioni di cui si ha bisogno, per giunta strutturate e pronte ad una consultazione mirata e intelligente. Specialmente se si tratta di normative, leggi, sentenze, circolari, quesiti con risposta, documentazione, il tutto interamente dedicato al mondo funerario.
Ora, tuttavia, c'è un punto di riferimento insostituibile per i professionisti del settore, sia nel pubblico che nel privato: è www.antigone.it, il portale italiano del settore funerario (figura 3): una miniera di informazioni in parte disponibile gratuitamente (ma con accesso sempre tramite password, da richiedere) e in parte a pagamento, accessibile a portata di clic del mouse (figura 4).
Sul sito www.antigone.it è possibile anche compilare on-line il questionario pubblicato sul numero scorso de "I servizi funerari" (figura 5). La ricerca, che si può condurre per mezzo di varie chiavi, conduce velocemente ad indici ipertestuali, con collegamenti a quesiti, leggi e circolari inerenti (figura 6) che si possono espandere a piacere (figura 7, 8 e 9).
Un bookmark davvero imperdibile per quanti lavorano nell'ambito funebre e cimiteriale.

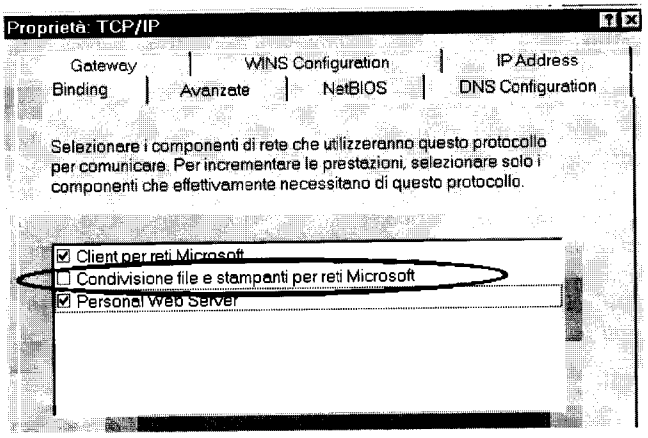

Figura 1

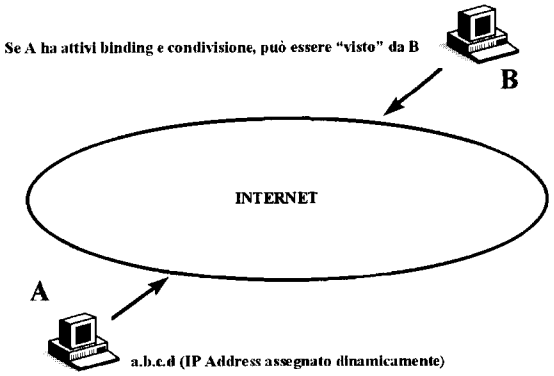

Figura 2

Figura 3

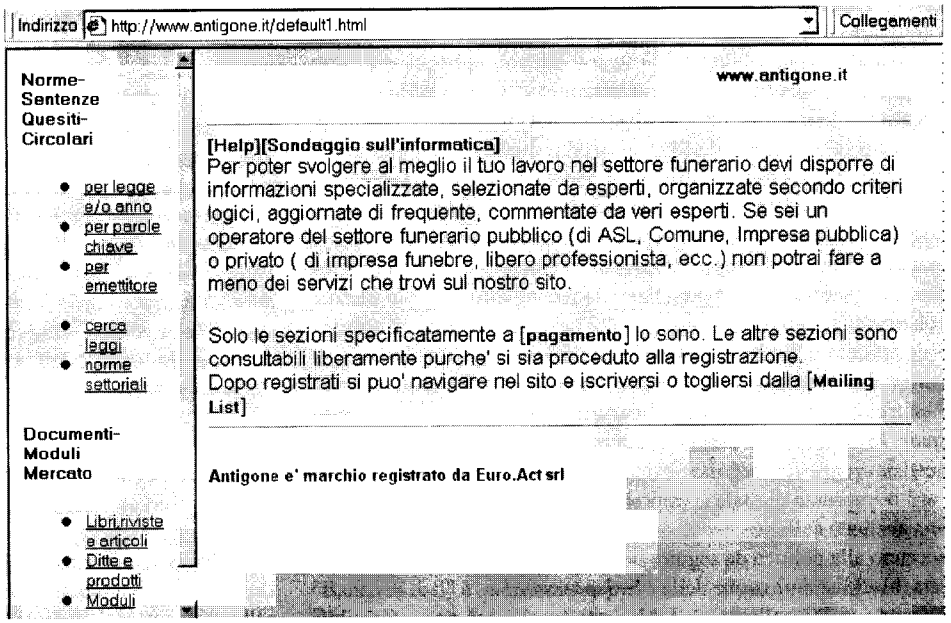

Figura 4

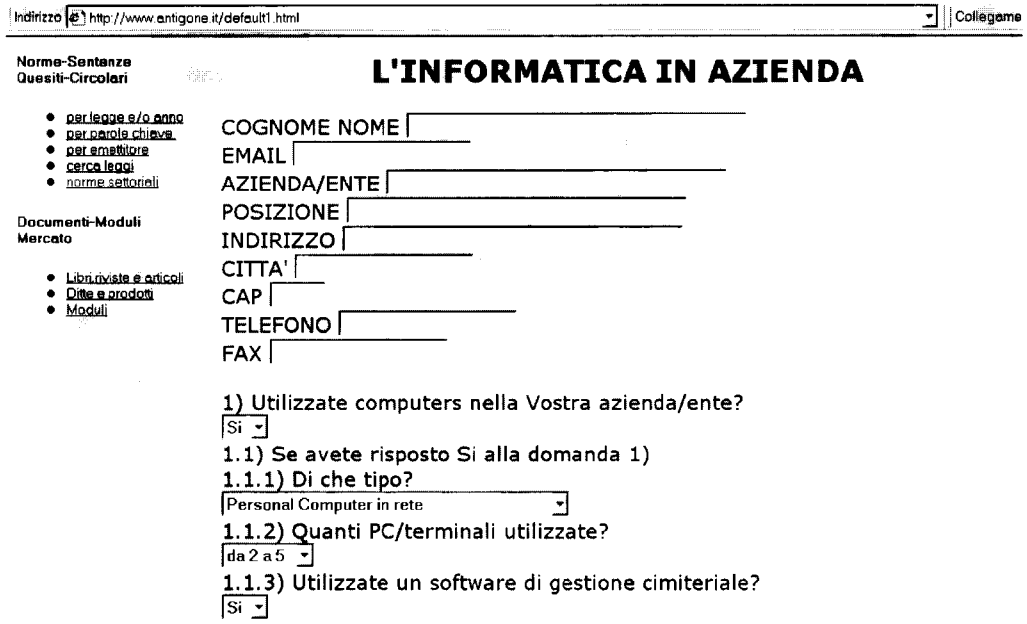

Figura 5

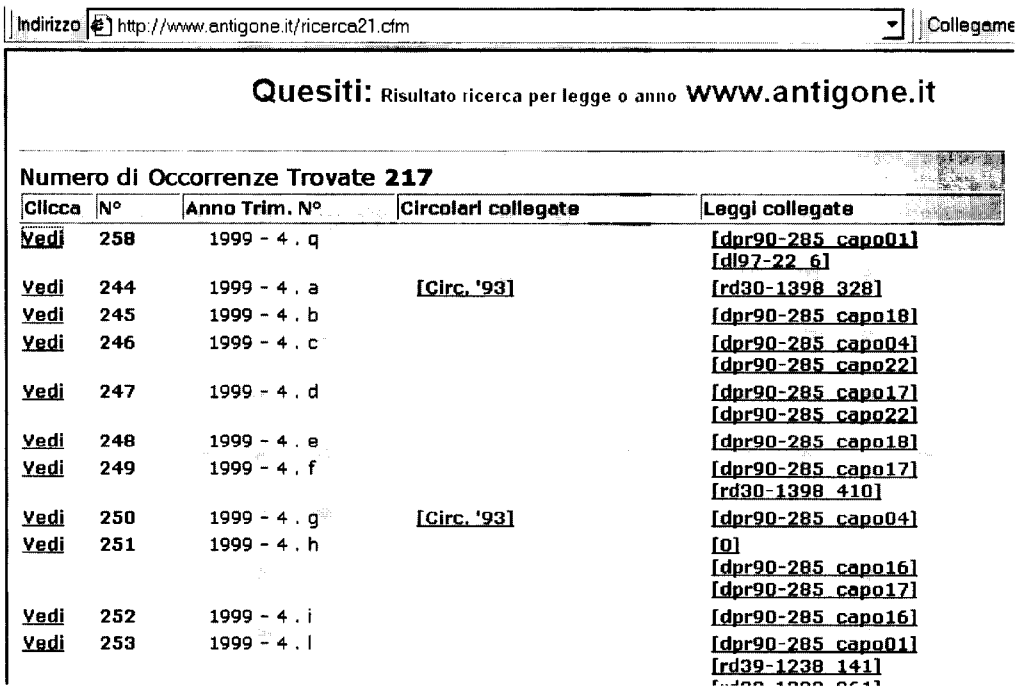

Figura 6

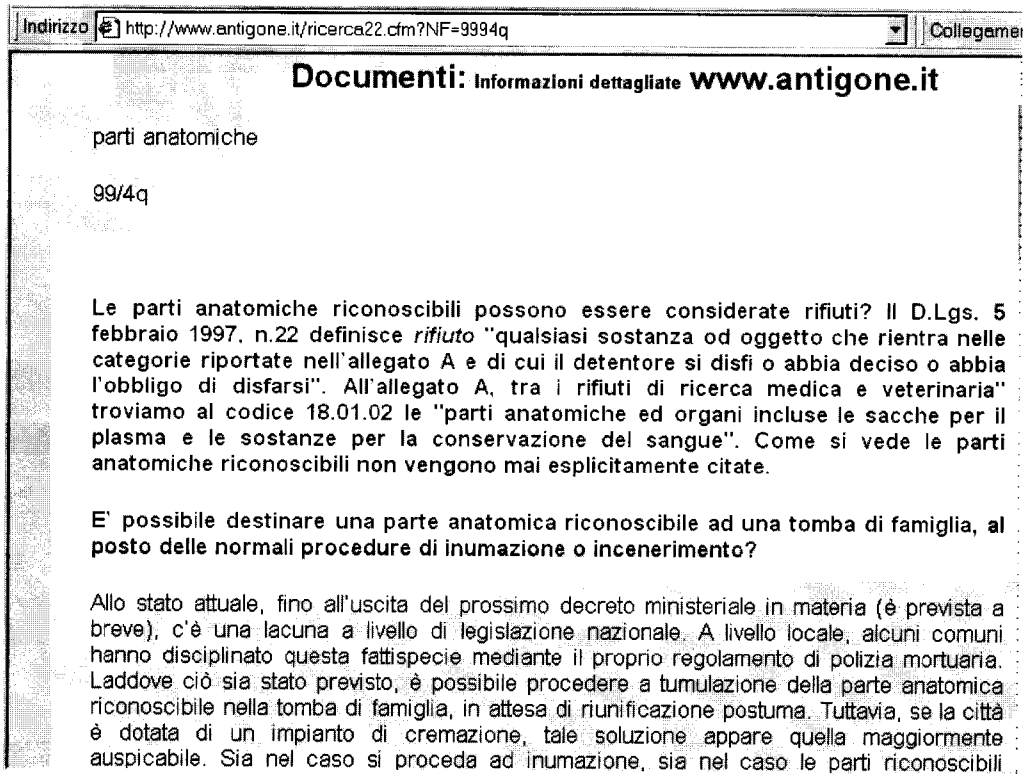

Figura 7

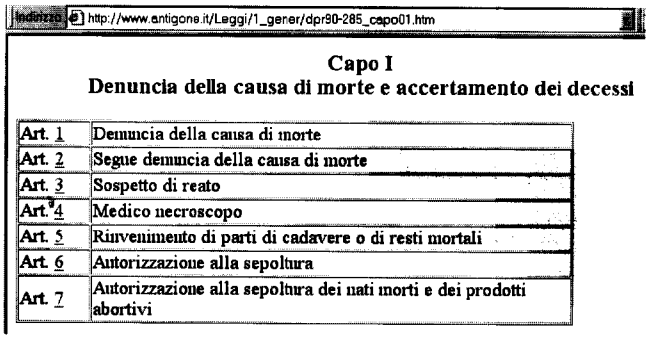

Figura 8

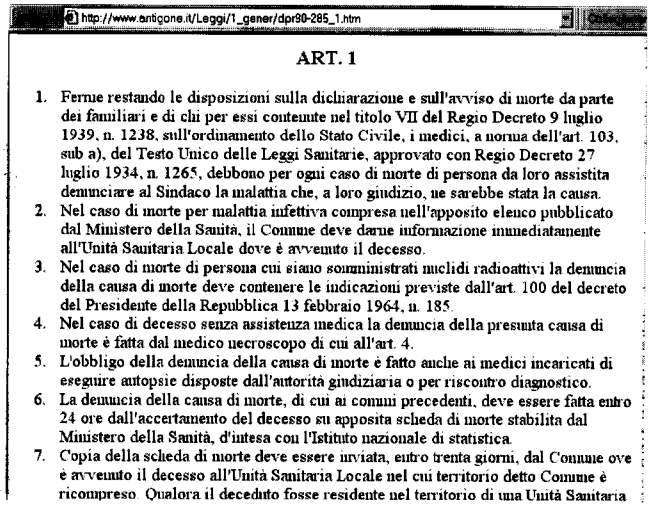

Figura 9