Legislazione

Dati personali un progetto da rifare

Sta per essere presentato alle Camere un disegno di legge del Governo sulla protezione della privacy, che ricalca in gran parte quello decaduto nella passata legislatura: un insieme confuso di norme inapplicabili

di Manlio Cammarata

Una legge per la tutela delle informazioni personali contenute nelle banche di dati ha iniziato, per l'ennesima volta, il suo cammino verso l'approvazione. Potrebbe essere colmato un ritardo di oltre vent'anni, rispetto ad altri paesi europei, e potrebbe essere finalmente sanata l'inadempienza delle disposizioni comunitarie. Ma il testo in discussione, anche se è coerente con i principi stabiliti a livello internazionale, sembra scritto più per creare problemi che per risolverne.

Il 5 dicembre scorso è stato inviato a tutti i ministeri uno schema di disegno di legge, emanato dal Ministero di Grazia e Giustizia il 27 ottobre. Si tratta del testo approvato dalla Camera dei Deputati nella scorsa legislatura, e poi arenatosi al Senato, con qualche aggiunta che non ne modifica lo spirito e la struttura.

Il vecchio disegno di legge era frutto dell'unificazione di due distinte proposte, basate sull'ormai antico «progetto Mirabelli» e sulla Convenzione di Strasburgo del 1981. L'Accordo di Schengen del 1985 e una Direttiva europea non ancora ufficialmente pubblicata sono tra gli altri punti di riferimento normativo. Frutto quindi di un iter travagliato, lo schema si presenta molto complesso e di non facile lettura. È suddiviso in trentasei articoli, raggruppati in dieci «capi» (il precedente disegno di legge era composto di nove capi e trentacinque articoli; è stato aggiunto un capo, composto da un solo articolo, che prevede l'emanazione di leggi delega da parte del Governo, per disciplinare aspetti particolari). Il titolo è: «Tutela delle persone rispetto al trattamento dei dati personali». Ecco qualche indicazione che emerge da una prima lettura.

Il Capo 1 contiene i principi generali e definisce che cosa si intende per «banca di dati», per «trattamento», per «dato personale», per «titolare», per «responsabile», per «interessato», per «comunicazione», per «diffusione», per «dato anonimo», per «blocco» e per «Garante» (art. 1). Appare a prima vista che la legge non fa differenze tra archivi cartacei e archivi elettronici, il che appare corretto sotto molti aspetti, ma già nel primo comma si legge un'espressione che desta qualche perplessità: *a) per «banca di dati» [si intende] qualsiasi insieme 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.* Non è chiaro che cosa sia questa «pluralità di criteri», forse si vuol dire che un sempice elenco in ordine alfabetico non è una banca di dati? Perché è chiaro che l'ordine alfabetico è un criterio che facilita il trattamento. Quest'ultimo è *b)... qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente 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* (la «cancellazione» è senza dubbio un «trattamento», ma è difficile definire tale la «distruzione», se non è cancellazione da parte del titolare).

I paragrafi successivi contengono alcune affermazioni importanti. Per dato personale si intende *qualunque informazione relativa a persona fisica, persona giuridica od ente, identificati o identificabili anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale*; mentre «l'interessato» è il soggetto al quale si riferiscono i dati. «Titolare» è *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente 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 invece *la persona fisica preposta dal titolare al trattamento di dati personali.* L'indicazione relativa alla sicurezza, come vedremo più avanti, è molto importante. È da notare poi la distinzione tra «comunicazione» (a soggetti determinati diversi dall'interessato) e «diffusione» (a soggetti indeterminati, anche offrendo la consultazione) dei dati personali.

A chi si applica?

Con l'art. 2 incominciano i problemi: *1. La presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato, ad eccezione di quello posto in essere da persone fisiche, a fini esclusivamente personali, sempreché i dati non siano destinati a una comunicazione sistematica o alla diffusione.* Dunque la mia agenda personale non ricadrebbe nel campo di applicazione della legge, perché i dati che contiene

non sono «destinati a una comunicazione sistematica o alla diffusione», ma mi resta il dubbio che, essendo i dati organizzati «secondo una pluralità di criteri», fra i quali la distinzione tra informazioni strettamente personali e informazioni relative al lavoro, io debba notificarne il possesso al Garante...

Il comma successivo complica le cose: *2. Il trattamento di dati personali svolto senza l'ausilio di mezzi elettronici o comunque automatizzati è soggetto alle disposizioni della presente legge limitatamente ai dati registrati in una banca di dati o che, all'atto della raccolta o nel corso di una successiva operazione, sono suscettibili di essere registrati in una banca di dati.* C'è qualcosa che non va: tutti i dati sono suscettibili di essere registrati in una banca di dati, quali sono esclusi? O questo scioglilingua è scritto male, o non significa nulla.

La legge non si applica al trattamento dei dati personali effettuato nell'ambito delle banche del Ministero dell'Interno, del Casellario giudiziale, degli uffici giudiziari e delle informazioni coperte dal segreto di Stato; più avanti questa esclusione è meglio delimitata e precisata per quanto riguarda il Ministero dell'Interno. *Poi non si applica al trattamento di dati personali di cui sia titolare un soggetto pubblico, effettuato in base ad espresse disposizioni di legge che prevedano specificamente il trattamento finalizzato alla protezione di interessi concernenti: a) la difesa o la sicurezza dello Stato; b) la pubblica sicurezza; c) la prevenzione, l'accertamento o la repressione dei reati.* È una materia delicatissima, sulla quale torneremo in un prossimo articolo, perché coinvolge in modo molto pesante due interessi contrapposti: la sicurezza pubblica e il diritto alla riservatezza, anche in relazione all'attività dei «servizi segreti».

Il comma successivo è un capolavoro dell'ingegneria legislativa italica nei suoi aspetti più perversi: *6. Oltre a quanto stabilito dagli articoli 6 e 20, le disposizioni degli articoli 4 e 7, commi 1, 2, 3 e 5, si applicano anche ai trattamenti di dati personali esclusi dal campo di applicazione della presente legge ai sensi dei commi 4 e 5 del presente articolo. Le disposizioni di cui ai predetti commi 1, 2, 3 e 5 dell'articolo 7 si applicano altresì ai trattamenti di cui al comma 1 del presente articolo.* Qui in sostanza si dice che alcuni articoli della legge (li vediamo più avanti) si applicano alla materia esclusa dalla legge, il che è alquanto contorto, per non dire illogico. Si aggiunga che esistono precise disposizioni ministeriali che impongono una maggiore chiarezza degli articolati.

Il Capo II è dedicato al trattamento dei dati personali. L'art. 3 stabilisce i casi in cui il trattamento è lecito, e cioè prima di tutto nell'attività degli enti pubblici per lo svolgimento dei loro compiti. Quando invece il trattamento dei dati è svolto da privati, è necessario il consenso espresso dell'interessato, a meno che il trattamento stesso non sia reso obbligatorio da una legge o da una normativa comunitaria, non avvenga nell'ambito dell'esecuzione di un contratto, riguardi dati provenienti da registri pubblici o comunque conoscibili da chiunque, sia finalizzato solo a ricerche scientifiche o statistiche, o nell'ambito della professione giornalistica o, infine, riguardi lo svolgimento di attività economiche, nel rispetto delle norme sul segreto industriale o aziendale.

L'art. 4 elenca i requisiti dei dati personali, che debbono essere: *a) trattati in modo lecito e corretto; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento conformemente a tali scopi; c) esatti e aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti.* Si tratta di disposizioni ineccepibili, che servono a evitare che, con la scusa di raccolte legittime, si possano acquisire o elaborare informazioni con scopi non legittimi.

Per i BBS è previsto un decreto

Il Capo IX dello schema di disegno di legge per la protezione dei dati individuali prevede una disciplina per le strutture telematiche. Nell'art. 34 si afferma che il Governo è delegato ad adottare *le modalità applicative della legislazione in materia di protezione dei dati ai nuovi mezzi di comunicazione e informazione per via telematica, anche al fine di salvaguardare il diritto all'informazione e i diritti degli utenti, e di individuare i compiti del gestore in rapporto ai servizi aperti al pubblico o riservati alla corrispondenza privata, e alle connessioni ai sistemi sviluppati su base internazionale.* Dunque la regolamentazione di BBS e simili, tanto discussa dopo le vicende dell'estate scorsa, dovrebbe trarre origine da qui. Ma l'articolo di delega non indica i principi ai quali si dovrebbe ispirare il decreto delegato, il che è strano. C'è un altro particolare non trascurabile: ammesso e non concesso che tra sei mesi questo schema di disegno di legge (o uno migliore!) si trasformi in legge, il Governo avrebbe ancora un anno e mezzo di tempo per emanare le norme delegate. Due anni di attesa non sono un po' troppi per una materia così

I dati «sensibili»

L'art. 5 (Categorie particolari di dati) elenca quelli che di solito vengono definiti «dati sensibili»: origine razziale ed etnica, convinzioni religiose, filosofiche, opinioni politiche, anomalie fisiche o psichiche, comportamenti sessuali, stato di salute. Si tratta delle informazioni più riservate che possono riguardare un individuo e la legge le tutela correttamente, stabilendo i casi in cui possono essere raccolte *con il consenso scritto dell'interessato e previa autorizzazione del Garante.* Norme particolari sono dettate anche nell'art. 16 per quanto riguarda l'elaborazione e la comunicazione dei dati sanitari, al fine di conciliare il rispetto dell'individuo con le esigenze della politica sanitaria e l'interesse pubblico in generale. È limitato anche il trattamento dei dati del Casellario penale. Quando il trattamento dei dati personali è svolto nell'esercizio della professione giornalistica non occorre il consenso dell'interessato e anche la diffusione è ammessa (art. 13).

L'art. 6 è particolarmente importante: *1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può avere per unico fondamento un trattamento di dati personali volto a definire il profilo o la personalità dell'interessato. 2. L'interessato può opporsi ad ogni altro tipo di decisione adottata sulla base del trattamento di cui al comma 1 del presente articolo...* Si sancisce il principio fondamentale, che nessuno può essere, in pratica, valutato, giudicato o condannato solo sulla base dei dati contenuti in un archivio.

Anche l'art. 7 riveste un interesse particolare, perché introduce criteri di sicurezza per la custodia e il trattamento dei dati, criteri che potrebbero (e dovrebbero) essere estesi a qualsiasi struttura informativa: *1. I dati personali oggetto di trattamento devono essere custoditi, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche della banca di dati, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di protezione, il rischio di una distruzione o perdita anche accidentale, di un accesso non autorizzato o di un trattamento non consentito o non conforme alle finalità della raccolta. 2. Con decreto del Presidente della Repubblica, da emanare [...] entro centottanta giorni dalla data di entrata in vigore della presente legge, sono individuate le misure minime di protezione da adottare ai fini di cui al comma 1 del presente articolo.* E ogni due anni le misure devono essere riviste in funzione del progresso tecnologico.

D'accordo sui principi, ma...

Entro un anno dalla data di entrata in vigore della presente legge, le regioni a statuto speciale e le province autonome di Trento e Bolzano adeguano i rispettivi ordinamenti ai principi fondamentali desumibili dalla legge medesima, che costituiscono norme fondamentali di riforma economico-sociale della Repubblica (art. 29).

Questo articolo dello schema di disegno di legge sulla protezione dei dati personali riassume nello stesso momento l'importanza e i limiti del testo. Il perché dell'importanza è chiaro: nel passaggio verso un modello di società in cui le informazioni contenute nelle memorie dei computer rivestono un ruolo essenziale per la struttura della società stessa, la difesa degli individui dal possibile abuso di queste informazioni costituisce un aspetto fondamentale della convivenza civile. Ma, ecco il limite, l'importantissima affermazione è contenuta in un articolo delle «Disposizioni transitorie e finali ed abrogazioni», cioè dopo il corpo normativo principale. Avrebbe dovuto essere scritta nell'articolo 1!

I principi ispiratori dello schema sono fuori discussione. Essi sono frutto di anni e anni di elaborazione, in Italia e all'estero, e il modello generale è ormai consolidato, anche se presenta soluzioni applicative diverse nei vari Stati. I Laender tedeschi dell'Assia nel '70 e della Renania-Palatinato nel '74 emisero le prime norme di questo tipo. L'elaborazione della legge federale tedesca, molto rigida, iniziò nel '71. L'Unione Europea ha ripetutamente sancito questi principi (l'ultima Direttiva sulla materia è in corso di pubblicazione), anche se dopo lunghe discussioni per contemperare gli interessi dell'industria con quelli della collettività. Il progetto italiano è conforme alle disposizioni comunitarie. Ma gli aspetti positivi si fermano qui.

Lo schema diffuso dal Governo il 5 dicembre '94 è una congerie di regole, eccezioni e contraddizioni. Gli obblighi di notifica al Garante dell'esistenza degli archivi e della trasmissione dei dati sono praticamente generalizzati. Se si pensa che il progetto della rete della pubblica amministrazione prevederà l'interconnessione di parecchie decine di migliaia di banche dati (solo le anagrafi comunali sono quasi diecimila) e che le imprese che possono rientrare nel campo di applicazione della legge sono probabilmente centinaia di migliaia, si può avere un'idea della mole di lavoro che dovrebbe essere svolta dall'ufficio del Garante.

Altri aspetti lasciano perplessi. Per esempio, si riconosce la fondamentale libertà dell'informazione giornalistica, escludendo da molti obblighi gli archivi dei giornali e dei giornalisti, fino ai limiti dell'arbitrio; si enunciano restrizioni sulla durata della conservazione dei dati che, se applicate alla lettera, porterebbero alla distruzione degli archivi storici. Per questi e altri aspetti si autorizza il Governo a emettere leggi delegate, ma che cosa potrebbe succedere nel periodo che trascorrerà tra l'entrata in vigore della legge e quella dei decreti legislativi?

Ovviamente gli obblighi del titolare della banca di dati non si esauriscono con l'osservanza delle norme di sicurezza. L'art. 8 del disegno di legge stabilisce che *Il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne previa notificazione al Garante* (ma tutti i trattamenti di dati, tranne quelli detenuti da persone fisiche per scopi personali, sono soggetti alla legge). Segue una lunga lista di informazioni che devono essere notificate. Il settimo comma afferma che il trattamento dei dati elencati dall'art. 5 (cioè dei dati riservati) *non può essere iniziato prima che siano decorsi quarantacinque giorni dalla data della notificazione. Durante tale termine, ovvero successivamente, il Garante può disporre opportune verifiche e l'adozione di misure o accorgimenti a garanzia dell'interessato, che il titolare è tenuto ad adottare.* L'art. 9 riguarda la nomina, da parte del titolare, di uno o più responsabili del trattamento dei dati.

I diritti dell'interessato

A questo argomento è dedicato il Capo III. L'art. 10 stabilisce che *1. La persona presso la quale sono raccolti dati personali deve essere previamente informata circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze, nei suoi confronti o nei confronti dell'interessato, di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 11; f) il nome e il domicilio o la residenza del titolare del trattamento e, se designato, del relativo responsabile. 2. Le disposizioni di cui al comma 1 non si applicano nei casi in cui le informazioni ivi previste impedirebbero la raccolta di dati necessaria per l'accertamento di illeciti o per l'irrogazione di sanzioni. 3. Nei casi in cui il trattamento presuppone il consenso dell'interessato, questo deve intendersi validamente prestato solo se è espresso liberamente e in forma specifica e se è stato rispettato il disposto del comma 1.* Le norme sembrano chiare, ma c'è qualcosa che non va nell'esposizione: chi è la persona «presso la quale» sono raccolti i dati?

Passiamo all'art. 11, che elenca i diritti dell'interessato. In sostanza, egli deve sapere se ci sono archivi che contengono dati che lo riguardano e i criteri della raccolta e del trattamento, può ottenere dal responsabile del trattamento la conferma dell'esistenza dei dati ed esigere *la cancellazione, il blocco o la trasformazione in forma anonima dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione, [...] l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati [...].* È da notare il punto 5, che risolve un problema che affligge molte persone: l'interessato ha diritto di ottenere *la cancellazione gratuita di dati utilizzati al fine di invio di corrispondenza o materiale pubblicitario.* La tutela dei diritti dell'interessato è molto ampia, fino alla facoltà *di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.* C'è da osservare che qui e in

La buona volontà

Martedì 13 dicembre, ore 17, Radio Tre: va in onda "2000", la bella trasmissione quotidiana condotta da Rossella Panarese. Si parla di banche dati e BBS con il magistrato Giovanni Buttarelli, dell'Ufficio legislativo del Ministero di Grazia e Giustizia, Paolo Nuti, editore di MC-link, e Franco Carlini del Manifesto. Buttarelli, che parla a titolo personale, descrive la futura legge sulle banche dati, manifestando non solo di avere le idee chiare sui problemi in discussione, ma anche la volontà di fare una buona legge.

Giovanni Buttarelli è, come si dice, un "addetto ai lavori", una delle persone che possono migliorare lo schema di disegno di legge che esaminiamo in queste pagine. E allora contiamo sulla sua buona volontà, e sull'apertura che ha dimostrato nella discussione radiofonica, per far giungere al Parlamento un testo scritto in modo più chiaro e con norme realmente applicabili.

Speriamo di poter ospitare un suo intervento sul prossimo numero di MCmicrocomputer.

altri punti si distingue tra «raccolta» e «trattamento», mentre nelle definizioni dell'art. 1 la raccolta è parte del trattamento. L'art. 12 elenca alcuni limiti ai diritti dell'interessato. Va segnalato il disposto dell'ultimo comma: *La comunicazione all'interessato di dati personali di carattere sanitario può essere effettuata solo per il tramite di un medico designato dall'interessato o dal titolare.*

Comunicazione e diffusione

Siamo arrivati al Capo IV, che regola la comunicazione e la diffusione dei dati (art. 13). Esse sono ammesse con il consenso dell'interessato, o se i dati provengono da pubblici registri, elenchi o atti conoscibili da chiunque, in adempimento a obblighi di legge o a normative comunitarie e, dato rilevante, nell'esercizio della professione giornalistica. È vietato comunicare e diffondere dati al di fuori delle finalità per le quali è stata inviata la notificazione, oppure per le quali è stata ordinata la cancellazione, o quando sia scaduto il tempo consentito per la loro conservazione. Inoltre *il Garante può vietare la diffusione di taluno dei dati relativi a singoli soggetti, od a categorie di soggetti, quando la diffusione si pone in contrasto con rilevanti interessi della collettività.* L'art. 14 elenca le cause di divieto: al di fuori dei limiti indicati nella notificazione, se ne sia stata ordinata la cancellazione, o se sia trascorso il periodo di tempo previsto, o per i motivi già visti di sicurezza pubblica e simili. L'art. 15 *(Comunicazione e diffusione dei dati nell'ambito o da parte della pubblica amministrazione)* assume un rilievo particolare nel momento in cui l'Autorità per l'informatica avvia il suo progetto di rete (ne abbiamo parlato in *Cittadini & Computer* sul numero del mese scorso), che fonda sullo scambio dei dati l'efficienza degli uffici e i rapporti con i cittadini. In sostanza lo scambio dei dati tra le pubbliche amministrazioni è ammesso quando è previsto da leggi o regolamenti, previa comunicazione al Garante, che può vietarlo se viola le disposizioni del disegno di legge. È evidente il rischio di conflitti tra le disposizioni di questo disegno di legge e le norme della pubblica amministrazione. Questo è un punto importante da discutere: tutto il funzionamento della pubblica amministrazione si fonda, in prospettiva, sullo scambio di dati tra i diversi uffici. Se si pensa che le amministrazioni interessate sono decine di migliaia, l'ufficio del Garante potrebbe essere sommerso da un tale diluvio di comunicazioni da restare completamente paralizzato. Sarebbe forse più opportuno che lo scambio dei dati all'interno della pubblica amministrazione fosse regolato con norme generali dall'Autorità per l'informatica nella pubblica amministrazione, prevedendo il ricorso al Garante solo per eventuali violazioni dei diritti dell'interessato.

La diffusione dei dati sulla salute e sulla vita sessuale (art. 16) è ammessa solo con il consenso dell'interessato, o su autorizzazione del Garante nel caso che sia indispensabile *per il trattamento sanitario dell'interessato o di terzi.* In ogni caso (art. 17) la comunicazione e la diffusione di dati anonimi sono permesse per finalità di ricerca o di statistica, mentre sono comunque permesse *quando siano necessarie per scopi concernenti la difesa dello Stato, la prevenzione o l'accertamento di illeciti o l'irrogazione di sanzioni, con l'osservanza delle norme che regolano la materia.*

Proseguiamo la nostra esplorazione con il Capo V, composto dal solo articolo 18. Esso in sintesi stabilisce che chiunque voglia trasferire dati personali all'estero deve darne notizia al Garante con trenta giorni di anticipo, che diventano quarantacinque nel caso di dati «sensibili». Il Garante deve accertare che nello stato di destinazione i dati godano di una protezione almeno pari a quella italiana. Una procedura analoga si applica per il trattamento sul nostro territorio di dati detenuti all'estero. E qui ci troviamo di fronte a norme la cui applicazione potrebbe essere molto problematica, a causa del progresso delle telecomunicazioni e della velocità di circolazione delle informazioni che esse implicano. Trenta giorni di anticipo per un'operazione che si può compiere in frazioni di secondo? Si aggiunga che l'art. 18 non esclude l'obbligo della notificazione per trasferimento all'estero o dall'estero di dati provenienti da pubblici registri, elenchi, atti, o documenti conoscibili da chiunque. Così, se qualcuno si collega alla nostra MC-link dall'estero via Internet e chiede l'elenco degli abbonati, il che avviene molte volte al giorno, bisogna notificare la cosa al Garante e attendere trenta giorni prima di rispondere...

L'art. 35 delega il Governo a legiferare su questo argomento, facendo supporre che gli estensori del testo si siano resi conto dell'inapplicabilità di alcune norme. Ma è una tecnica legislativa molto strana: si detta una norma, poi si delega il Governo a farne un'altra contraria, ponendo, al limite, anche un problema di legittimità costituzionale della norma delegata.

Il Garante

Giunti al Capo VI, ci imbattiamo finalmente nella figura del Garante per la protezione dei dati. Leggiamo l'art. 19: *1. È istituito il Garante per la protezione dei dati. 2. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. 3. Il Garante è organo collegiale costituito dal presidente e da quattro membri, nominati con decreto del Presidente della Repubblica, su proposta formulata d'intesa tra loro dai Presidenti del Senato della Repubblica e della Camera dei deputati. Il presidente e i membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza nelle materie dell'informatica e del diritto. 4. Il presidente e i membri durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i membri non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive [...].* Si tratta quindi di un organo simile alle autorità per la concorrenza o per l'informazione, con compiti molto ampi. Deve infatti tenere un registro delle notifiche ricevute, controllare se i trattamenti di dati rispondono ai requisiti di legge e segnalare ai titolari le modifiche eventualmente necessarie, accogliere le segnalazioni e i reclami degli interessati, adottare i provvedimenti previsti dalla normativa, denunciare all'autorità giudiziaria i fatti configurabili come reati perseguibili d'ufficio, vietare il trattamento dei dati, o disporne il blocco in caso di possibili pregiudizi per uno o più interessati e così via.

Oltre a queste mansioni di sorveglianza, il Garante ha anche compiti di più vasta portata, come *segnalare al Governo l'opportunità di provvedimenti normativi richiesti dall'evoluzione del settore, e anche promuovere nell'ambito di categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti [...] e contribuire a garantirne la diffusione e il rispetto; curare la diffusione tra il pubblico dell'attività svolta, della conoscenza delle norme che regolano la materia e delle relative finalità,*

Le opinioni dei giuristi

Lo schema del 27 ottobre '94 è in gran parte identico al disegno di legge, approvato dalla Camera nel '93 e poi decaduto con la fine della legislatura, che aveva suscitato non poche critiche. Per Carlo Sarzana di Sant'Ippolito, il «padre» della legge 547 sui crimini informatici, anche i criteri di sicurezza delle banche di dati pubbliche dovrebbero essere indicati dall'Autorità per l'informatica nella pubblica amministrazione, oltre a quelli tecnici: «A mio avviso - afferma Sarzana - le indicazioni dei criteri tecnici di sicurezza dei dati, anche personali, contenuti nei sistemi informatici pubblici non possono non spettare all'AIPA quale organo indipendente, che dovrebbe sovrintendere a tutta la materia della sicurezza informatica pubblica. È assolutamente indispensabile, e risponde ad elementari criteri di razionalità, che vi sia un'unica autorità nazionale investita del compito di provvedere in tema di sicurezza dei sistemi informativi pubblici, con qualche motivata esclusione per particolari sistemi».

Un altro magistrato, il consigliere della Corte di Cassazione Renato Borruso, è ancora più severo. Borruso, che è stato tra i fondatori del CED della Corte ed è considerato tra i massimi esperti di informatica giuridica, ha fatto letteralmente a fettine il disegno di legge, in un lungo articolo pubblicato dalla rivista «Informatica & Documentazione» nn. 1-2 del 1994. L'insigne giurista ha criticato «la sorprendente estensione della tutela dalle banche dati informatiche a quelle cartacee»; ha osservato che il limite all'applicazione della legge ai dati detenuti dalle persone fisiche a fini personali è «insufficiente e oscuro»; si è soffermato, fra l'altro, sull'«inquietante disciplina prevista per i dati sanitari», rilevando alcune contraddizioni, e ha concluso: «Le critiche che ho già esposte [al disegno di legge] mi sembrano sufficienti ad augurarci che esso non si tramuti mai in legge».

Ha replicato, sulla stessa rivista, il magistrato Giovanni Buttarelli, dell'Ufficio legislativo del Ministero di Grazia e Giustizia, che viene da molti indicato come l'estensore materiale del disegno di legge. Buttarelli ha tracciato la storia del provvedimento (ricordiamo che la discussione verteva sul precedente DDL) e ha riconosciuto che «la fretta con la quale la Camera ha ultimato l'esame degli emendamenti ha determinato alcune disarmonie del testo» (disarmonie che sarebbero state eliminate nell'attuale versione). In sostanza, secondo Buttarelli, il testo non fa altro che recepire le disposizioni dell'Unione Europea, e «l'interprete dovrebbe evitare di alimentare eccessivi dubbi interpretativi o di patrocinarne la modifica in direzioni non praticabili».

Carlo Sarzana di Sant'Ippolito

nonché delle misure di sicurezza di cui all'articolo 7. Il secondo comma dell'art. 20 elenca i poteri del Garante per l'espletamento dei suoi compiti, fra i quali la richiesta di informazioni ai titolari o ai responsabili delle banche di dati, e anche ispezioni e controlli. Deve indicare le modifiche da compiere per i trattamenti che non rientrino nelle norma e comunicare l'esito delle sue azioni agli interessati che abbiano richiesto gli accertamenti.

L'art. 21 determina le caratteristiche dell'Ufficio del Garante, che può essere composto al massimo da cinquanta persone: poche, pochissime, se si considera il numero di banche dati già esistenti e la prevedibile crescita nel prossimo futuro.

Saltiamo, per questa volta, il Capo VII, relativo alle sanzioni, per occuparci del Capo VIII, dedicato alle disposizioni transitorie e finali. Esso contiene (art. 29) un'affermazione molto importante: le disposizioni di questa legge *costituiscono norme fondamentali di riforma economico-sociale della Repubblica.* Si riconosce quindi la rilevanza del trattamento dei dati individuali per il progresso della vita civile.

Problemi aperti

La legge entrerà in vigore centoventi giorni dopo la pubblicazione sulla Gazzetta Ufficiale: un termine non eccessivo, se si pensa che molte strutture dovranno rivedere profondamente la loro organizzazione. Entro lo stesso termine dovranno essere compiute le notificazioni previste dagli articoli 8 e 18 per i trattamenti iniziati prima dell'entrata in vigore della legge, ma a questi non si applicano le norme che prescrivono il consenso dell'interessato. Resta però la possibilità di esercitare i diritti previsti dall'articolo 11 (accesso, rettifica, cancellazione, ecc.) e dall'art. 22 (tutela amministrativa e giurisdizionale).

L'art. 32 modifica l'art. 10 della legge del 1 aprile 1981 sulla banca dati del Ministero dell'Interno, ponendo anche questa sotto il controllo del Garante: *Il controllo sul centro elaborazione dati è esercitato dal Garante per la protezione dei dati, nei modi previsti dalla legge e dai regolamenti.* Per gli interessati che vengano a conoscenza dell'esistenza di dati che li riguardano c'è la possibilità di chiedere alla magistratura di compiere accertamenti e ordinare rettifiche, integrazioni, cancellazioni o trasformazioni in forma anonima. Si tratta di una serie di norme molto importanti, perché la legge dell'81 presenta gravi lacune nella tutela dei diritti dell'interessato. È una materia delicatissima, perché deve conciliare le esigenze di protezione dell'ordine pubblico con la tutela dei diritti dei singoli: torneremo presto sull'argomento.

Il Capo IX, *Disciplina integrativa,* delega il Governo *ad adottare, entro diciotto mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni modificative ed integrative della legislazione in materia di protezione dei dati personali.* Le materie previste riguardano il trattamento di dati a fini storici, di ricerca e statistica, con particolare riferimento alla durata della loro conservazione, limiti e condizioni per il trattamento di informazioni consistenti in un numero di identificazione personale e modalità di diffusione dei dati nell'ambito della professione giornalistica. Sono previste norme delegate anche per la banca dati del Ministero dell'Interno e per i dati riguardanti la sicurezza pubblica e l'attività giurisdizionale, oltre che per le strutture telematiche (se ne parla nel riquadro).

A questo punto non resta che chiedersi se questo progetto soddisfi le attese e risolva i molti problemi aperti. La risposta è in parte negativa, perché molte disposizioni non sono adeguate allo stato della tecnologia e troppi sono i vincoli, più burocratici che sostanziali, posti alla raccolta e al trattamento dei dati. Proteggere i dati sensibili è giusto, come è opportuno liberare i cittadini dall'impressione di essere schedati in tutti i modi possibili e al di fuori di qualsiasi controllo. Ma per ottenere questi risultati si possono trovare formule meno onerose e, soprattutto, si possono scrivere leggi meno aggrovigliate. Quindi più facili da rispettare e far rispettare. MC

Apparecchi medicali con programmi pirata

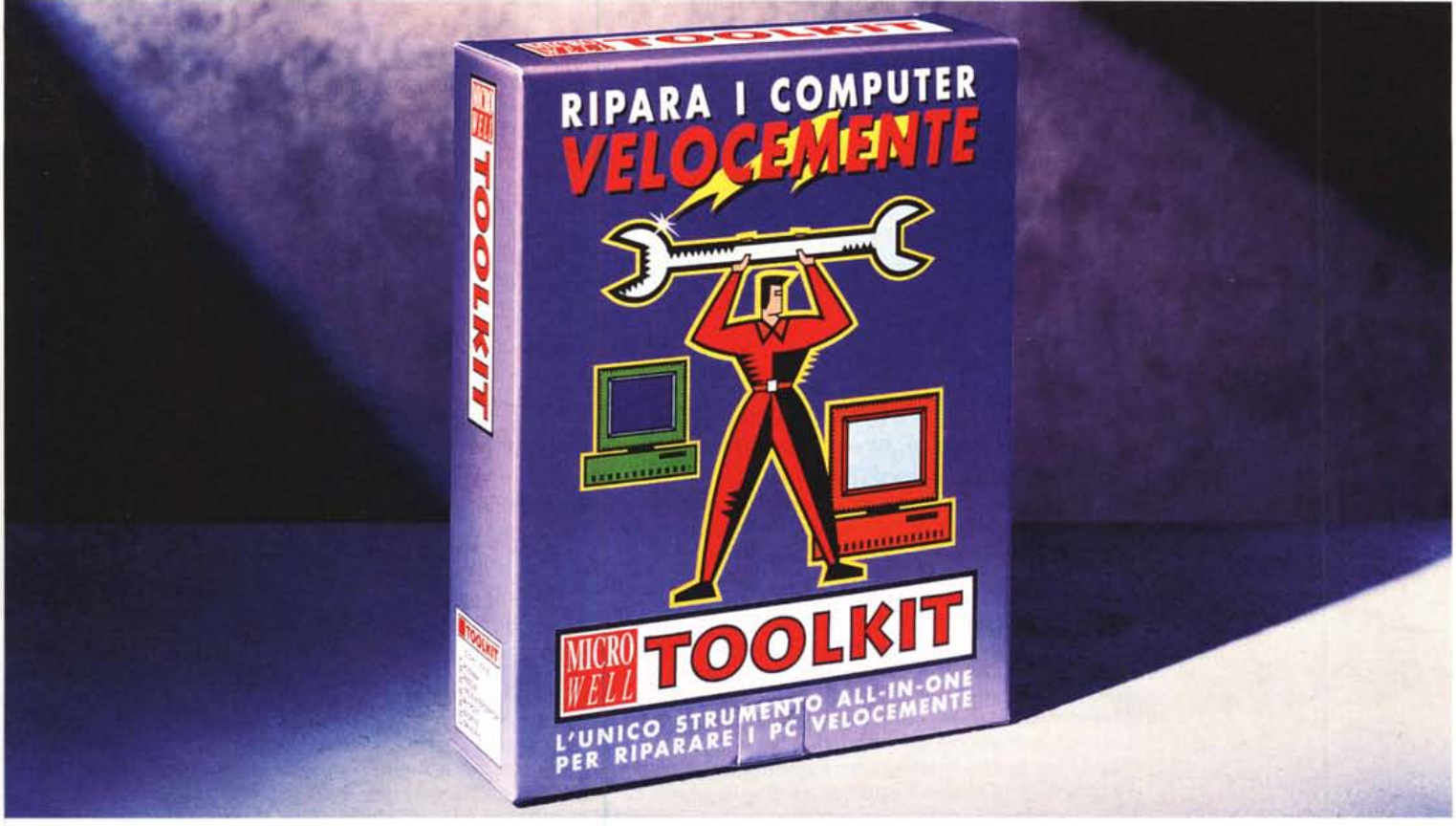
Baschi Verdi, operazione EPROM

La Guardia di Finanza di Roma, in un'indagine condotta in tutta Italia, ha scoperto un'organizzazione che copiava i contenuti delle EPROM di apparecchiature per analisi cliniche. Un'industria vendeva quindi gli apparecchi provvisti di un firmware illegale. Sembra una notizia qualsiasi, e invece presenta alcuni aspetti interessanti.

Per la prima volta, per quello che si sa, il DL 518 sulla protezione dei diritti degli autori del software viene applicato non alla copiatura abusiva di programmi su dischetti o CD- ROM, destinati a una vasta diffusione, ma in un settore molto più ristretto, che richiede apparecchiature e tecnologie molto più sofisticate.

Il secondo punto da considerare, e apprezzare, è che i «Baschi Verdi» del II Gruppo di Roma sono stati diretti da un PM esperto di informatica, Giuseppe Corasaniti, e hanno affidato le perquisizioni a specialisti del Corpo. Si legge nel comunicato «Le apparecchiature sequestrate sono molto sofisticate e sono dirette ad analisi cliniche molto complesse. Valutata appieno questa circostanza i militari, con il concorde parere dell'Autorità Giudiziaria, hanno provveduto a sequestrare le macchine lasciando, però, la facoltà d'uso delle stesse agli utenti».

Dunque la Guardia di Finanza di Roma, disponendo di personale specializzato, ha acquisito sul posto le prove dell'illecito e non ha quindi dovuto interrompere l'attività dei laboratori che utilizzavano, probabilmente in buona fede, le apparecchiature con il programma copiato. Perfetto! MC



COMPUTER IN TILT ?
TOOLKIT, SOLUZIONE IMMEDIATA.

TOOLKIT: il sistema all in one più avanzato e completo per la manutenzione del computer.
Un tecnico EDP, un tecnico di manutenzione, un assemblatore non può farne a meno.
È la sua task force per risolvere in brevissimo tempo qualsiasi problema, senza alcun altro ausilio che…due cacciaviti.

EZ DRIVE: dischi fissi no problem.
Installa, configura e formatta qualsiasi disco fisso IDE di qualsiasi capacità, in 60 secondi. Scopre ed elimina automaticamente i virus dei settori di caricamento. Permette di installare fino ad un massimo di 4 dischi fissi di qualsiasi tipo (IDE, ESDi, ST506/412) in aggiunta ad un HDD SCSI. Scavalca le limitazioni del DOS e permette di avere fino a 2 GB in un'unica partizione senza l'ausilio della memoria.
Assicura compatibilità tra il disco fisso ed il BIOS. Possiede diagrammi che descrivono la collocazione dei jumper per molti dei più usati dischi fissi.

RESCUE: I dati salvati.
È il primo programma che risolve l'inabilità del DOS a leggere dischi fissi e dischetti con danni fisici, recuperandone interamente i dati in 60 secondi. Recupera tutti i tipi di file: testo, exe, grafici o intere sottodirectory, fino ad un massimo di 700 file per sottodirectory. Funziona su floppy da 360, 720, 1/2, 1.44 e 2.88Mb e su dischi rigidi MFM, ESDI, SCSI, IDE fino a 2.8 Gigabyte.
Basta con l'odiosa frase "Annulla, Riprova, Ignora,Tralascia".

VIRUS INTERCEPTOR: lo specialista.
Il nostro paese è il maggior produttore mondiale di virus, che non vengono riconosciuti dagli antivirus stranieri. Virus interceptor è stato pensato specificatamente per il mercato italiano, per individuare i virus con grande precisione in tutto il territorio nazionale e quindi effettuare una pulizia molto accurata.
Il programma ha inoltre la possibilità di riconoscere i virus mutanti e le nuove varianti dei ceppi virali più diffusi.

PC CHEK: diagnosi in tempo reale.
Verifica la configurazione hardware identificandone tutti i componenti per poi sottoporli a test specifici. Permette il controllo esaustivo di processore, coprocessore, DMA, CMOS, Clock, Timer, interruzioni, tutte le aree di memoria incluso la cache esterna, FDD, HDD. Porte seriali e parallele, keyboard, mouse, video, includendo SVGA e VESA, memoria video ecc. Ha anche una sezione Multimediale intelligente che verifica CD ROM e schede sonore. Consente il formattamento a basso livello anche dei dischi IDE. Consente la stampa del "rapporto d'intervento", un burn-in dinamico fino a 99H, la selezione dei test in modo bach, l'elenco dei codici POST.

MINIPOST: sblocca i PC senza vita, subito.
Una scheda unica per individuare le ragioni di mancata inizializzazione del computer. Inserendo la scheda nel computer ed accendendolo, istantaneamente attraverso un codice d'errore, la scheda mostrerà PERCHÉ il computer è bloccato, anche se lo schermo del monitor rimane nero. Diagnostica tutti i computer XT, AT, ISA e EISA. 4 Led indicano lo stato della corrente elettrica erogata dall'alimentatore. Incorpora un display digitale che visualizza i codici POST.
Il manuale, molto completo e di facile consultazione, include le tabelle dei codici di errore delle BIOS più comuni.

Solo per un numero limitato di copie il TOOLKIT è in offerta a L. 649.000 anzichè L. 949.000. Approfitta subito di questa straordinaria offerta!

Telefona oggi stesso
(02) 8910832
FAX (02) 8135305

MICROWELL srl Via Benevento, 3 - Milano 20142

MasterCard VISA CartaSì

Supporto tecnico gratuito!
Disponibilità immediata! Prestazioni Garantite!

Telefona subito od invia questo coupon compilato al Fax 02-8135305 per ottenere subito gratuitamente la documentazione tecnica con la soluzione per: ☐ Perdita di dati/Crash del disco ☐ Computer bloccato ☐ Problemi intermittenti ☐ Surriscaldamento ☐ Conflitti di IRQ/DMA

Nome.....
Società.....
Indirizzo.....
Città.....Cap.....Prov.....
Tel. .....Fax .....

IL NUMERO DI TELEFONO È NECESSARIO

MCM