CAMERA DEI DEPUTATI N. 780

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

ROTIROTI, POTÌ, ARTIOLI

Disciplina dell'uso dei sistemi informativi personali

Presentata il 18 maggio 1992

ONOREVOLI COLLEGHI ! — Il crescente sviluppo dell'informatica e la susseguente costituzione di numerose banche dati personali destinate agli scopi più diversi, rende sempre più attuale ed urgente l'esigenza di un'adeguata tutela dei diritti della persona ed in particolare della cosiddetta *privacy* individuale. Per indicare il livello di espansione delle « banche », sia pubbliche che private, destinate a raccogliere dati personali basta ricordare, a titolo esemplificativo, quelle consistenti in semplici elenchi di abbonati alla RAI-TV od alla SIP o di utenti di ENEL, acqua e gas; quelle più complesse di utenti INPS ed INAM, quelle delle anagrafi comunali o tributarie per arrivare alle « banche » dell'Amministrazione giudiziaria, del Ministero dell'interno, dei centri di reclutamento delle forze armate per non parlare di quelle sui dipendenti delle grandi amministrazioni, industrie, centri commerciali, di quelle delle banche ed assicurazioni sulla propria clientela, o di ordini professionali, associazioni e sindacati sui propri iscritti.

Tutti, di per sé, utilizzi ovvii di strumenti tecnici ormai nell'uso comune. Un primo campanello d'allarme suonò, nel dicembre 1981, quando in base all'articolo 8 della legge 1° aprile 1981, n. 121, di riforma dell'ordinamento dell'amministrazione della pubblica sicurezza, si ventilò il rischio di trovarsi « schedati » senza saperlo: la norma prevede che « ogni amministrazione, ente, impresa, associazione o privato che per qualsiasi scopo formi o detenga archivi magnetici nei quali vengano inseriti dati od informazioni di qualsivoglia natura concernenti cittadini italiani, è tenuta a notificare l'esistenza dell'archivio al Ministero dell'interno ».

Norma di sapore evidentemente garantistico che riguarda direttamente aziende,

professionisti, uomini d'affari, istituti finanziari ma li coinvolge al tempo stesso in qualcosa che può divenire un enorme diritto di prelievo da parte del pubblico potere e che può violare la *privacy* se non si dà un seguito adeguato e tempestivo a quanto previsto nel medesimo articolo di legge: « entro il 31 dicembre 1982 il Governo informerà il Parlamento degli elementi così raccolti ai fini di ogni opportuna determinazione legislativa a tutela del diritto alla riservatezza dei cittadini ».

Preoccupazioni e sospetti nacquero anche all'atto della compilazione della scheda del censimento nazionale nel senso che degli elaboratori elettronici potessero scrutare l'individuo seguendolo dalla culla alla tomba in una moderna ed anomala forma di *welfare state.*

Indiscutibilmente si possono profilare ipotesi di pericoli, ibride commistioni, eventuali forme di spionaggio nel nome della razionalità, efficienza e funzionalità, che pur sono necessarie.

Recentemente a Milano ad opera della *Etas-Kompass* si è costituita la banca dati *Kompass* per rispondere alle esigenze di tempestività nel mondo delle ricerche di informazione: sono state già inserite 200.000 aziende a livello europeo di cui 26.000 operanti in Italia.

Analoga attività svolge a Padova il *Cerved,* con il determinante supporto operativo delle camere di commercio, fornendo i più avanzati mezzi di elaborazione automatica per trattare dati emergenti dalle attività economiche e sociali erigendoli, dove è possibile, a sistema integrato di informazione e coordinando iniziative intese ad arricchire il patrimonio *software* applicativo e divulgativo. Nel contempo il *Cerved* è collegato a un'agenzia di informazioni commerciali a livello internazionale, la *Dun and Bradstreet,* che possiede il monopolio delle informazioni dei paesi d'oltre oceano e sembra abbia colleganze con servizi d'informazione statali americani.

Non a caso, in relazione alla delicatezza della problematica di cui trattiamo, a Roma sin dal febbraio 1981 si è svolto un seminario, organizzato dalla IBM-Italia in collaborazione con l'associazione *il Mulino* di cui gli atti, quanto mai interessanti, sono disponibili. La stessa Camera dei deputati ha pubblicato un pregevole volume sulle « banche dati e tutela della persona » comprendente testi di 16 Paesi, documenti, ricerche e proposte di autorevoli organizzazioni internazionali.

Da quanto precede si evidenziano preoccupazioni di situazioni in palese contrasto con le elementari norme di tutela dei diritti dell'uomo per quanto concerne la riservatezza; oltre che potersi configurare un vero e proprio attentato alla segretezza professionale. Non è un mistero che particolari istituti e studi professionali negli archivi contengono una svariata gamma di dati sul singolo cliente: fido bancario, protesti ricevuti, capacità e consistenza imprenditoriale; redditività, atti di transazioni valutarie, commerciali e di immobili, valori patrimoniali, eccetera.

Il rischio è quello di trovarsi schedato senza saperlo. Le banche dati e gli archivi elettronici di enti vari stanno diventando sempre più di uso comune ed acquistando un ruolo rilevante. Si costituiscono delle banche dati a cui il cittadino non può accedere ed è impossibile una verifica e, se del caso, una necessaria rettifica per eventuali, fortuiti o voluti, errori in relazione al fatto della possibile manipolazione dei dati raccolti, che possono travisare la qualità dell'informazione.

Occorre quindi, una specifica tutela giuridica della riservatezza dall'assalto dell'elettronica e dal possibile inquinamento dell'elaboratore. Siamo dinanzi ad una vera e propria carenza dei pubblici poteri preposti, una lacuna che si deve colmare al più presto per non restare indifesi di fronte all'informazione organizzata. L'Italia è l'unico Paese europeo privo di una normativa e manca anche una specifica regolamentazione dei sistemi di scambio internazionale.

Il nostro Paese potrebbe diventare il porto franco elettronico di terminali di dati per disinvolti giochi commerciali, industriali, finanziari e politici.

Si è dinanzi ad un delicato problema di tutela della riservatezza dei dati rac-

colti, da chiunque, in relazione alla *privacy* del cittadino. Si tratta di applicare la tutela della personalità prevista dagli articoli 2, 3 e 13 della Costituzione in relazione anche alla Dichiarazione universale dei diritti dell'uomo del 1948 e agli articoli 8 e 10 della Convenzione europea sulla salvaguardia degli stessi diritti, del gennaio 1981, firmata dall'Italia nel febbraio 1983.

In quest'ottica è nata una nuova scienza: la giuscibernetica. Come riportato dalla stampa, secondo il censimento fatto dal Ministero dell'interno, al dicembre del 1982 risultavano esistenti 105.739 archivi elettronici; il 90 per cento dei quali censisce non più di 100.000 individui. Il tutto per un totale di 250 milioni di schede personali.

Se si dovesse procedere ad un coordinamento ed al collegamento, a mezzo terminali, di tutti questi centri elettronici, la risultante sarebbe la costituzione di una maxicentrale di informazioni con conseguenze difficilmente immaginabili.

È proprio in relazione a queste potenziali eventualità che è quanto mai inspiegabile l'indolenza e la lentezza dei pubblici poteri preposti. D'altro canto si è convinti, e la legge lo indica, che non è bastevole e sufficiente a garantire la massima tutela alla riservatezza del cittadino quanto già sancisce la legge n. 121 del 1981: occorrono strumenti legislativi precisi e vincolanti, rigorosi controlli, per impedire possibili usi distorti.

Onorevoli colleghi, con la presente proposta di legge si intende dotare la nazione di uno strumento indispensabile, a premessa della ulteriore definizione di quelle prassi e normative discendenti che il progresso della tecnica e l'evoluzione socioculturale della società rendono improcrastinabile, pena il grave rischio di rendere vani gli stessi princìpi ispiratori della nostra Costituzione.

PROPOSTA DI LEGGE

—

ART. 1.

1. Nella presente legge il termine « sistema informativo » indica tutte le componenti e le operazioni di un processo di elaborazione dati, automatico o manuale, contenente informazioni personali, ed il nome o il codice caratteristico di un individuo, ed altri elementi particolari di identificazione.

2. Il termine « informazioni personali » indica tutte le informazioni che descrivono, localizzano o indicizzano qualsiasi dato relativo ad un individuo, quali educazione, transazioni finanziarie, storia medica, storia criminale, *curriculum* di impiego; o che forniscono dati relativi alle caratteristiche personali, quali impronte digitali, profilo vocale, fotografie o atti effettuati o subiti dall'individuo; o la registrazione della sua presenza, appartenenza od affiliazione ad organizzazioni, attività od istituzioni.

3. Il termine « soggetto di dati » indica un individuo le cui informazioni personali sono inserite e indicizzate in un sistema informativo e possono essere reperite in corrispondenza del suo nome, codice caratteristico, o altri elementi particolari di identificazione.

4. Il termine « disseminazione » indica l'attività consistente nel rilasciare, trasferire o comunicare informazioni, oralmente, o per iscritto o con mezzi elettronici, o con qualsiasi altro mezzo.

5 Il termine « organizzazione » indica enti dello Stato, delle regioni, delle province, dei comuni; qualsiasi entità pubblica o privata impegnata in affari industriali, commerciali ed altri simili.

6. Il termine « cancellare » indica l'attività consistente nell'eliminare informazioni in maniera permanente da qualsiasi archivio informativo di un'organizzazione.

ART. 2.

1. Ogni organizzazione che mantiene un sistema informativo nel quale sono incluse informazioni personali deve:

a) raccogliere, mantenere, usare e disseminare solo informazioni specificatamente pertinenti alle esigenze di un dichiarato ed appropriato compito dell'organizzazione;

b) raccogliere informazioni, per quanto possibile, solo direttamente dal soggetto di dati;

c) stabilire categorie di personale addetto al sistema informativo da abilitare al trattamento dei diversi livelli di confidenzialità dei dati;

d) mantenere le informazioni nel sistema con la precisione, completezza, aggiornamento e pertinenza necessari ad assicurare la massima equità nelle determinazioni derivanti dalle informazioni predette e relative al soggetto di dati;

e) non compiere alcuna disseminazione verso altri sistemi, o a individui diversi dal soggetto di dati a meno che l'altro sistema od individuo non garantiscano l'adeguato livello di riservatezza e non specifichino che l'uso dell'informazione è relativo ad esigenze conformi a quanto previsto alla lettera *a)*;

f) non trasferire alcuna informazione personale ad organizzazioni straniere senza autorizzazione del soggetto di dati;

g) garantire a qualsiasi soggetto di dati di nazionalità straniera, residente in Italia o meno, gli stessi diritti dei cittadini italiani;

h) mantenere una lista di tutte le organizzazioni, o categorie di impiegati, aventi regolare accesso alle informazioni personali del sistema informativo;

i) mantenere una registrazione completa ed accurata, comprendente identità, scopo e data, di ciascun accesso a qualsiasi informazione personale del sistema

informativo, compiuta da organizzazioni o persone che non hanno autorizzazione stabile a regolare accesso;

l) stabilire regole di comportamento, ed assumere le opportune iniziative per informare le persone addette al sistema informativo di tali regole, del contenuto della presente legge, e delle conseguenze personali delle possibili violazioni di essa;

m) stabilire appropriati sistemi di salvaguardia organizzativi, operativi e tecnici, contro ogni ragionevole prevedibile violazione alla sicurezza delle informazioni personali;

n) evitare di raccogliere alcuna informazione relativa ad un soggetto di dati su argomenti relativi alle sue credenze, affiliazioni ed attività politiche e religiose;

o) notificare l'esistenza dell'archivio al Ministero dell'interno nei termini delle disposizioni di cui al quarto comma dell'articolo 8 della legge 1° aprile 1981, n. 121.

ART. 3.

1. Ogni organizzazione che mantiene un sistema informativo che dissemina dati statistici o di ricerca, basati su informazioni personali, derivanti dal proprio sistema o da quelli di altre organizzazioni, deve:

a) rendere disponibili a qualsiasi soggetto di dati la metodologia ed i materiali necessari a convalidare le analisi statistiche;

b) evitare di rendere disponibile alcun materiale per analisi indipendenti, senza garanzia che alcuna informazione personale non venga usata in modo da causare pregiudizio al soggetto di dati interessato.

2. Nessuna organizzazione nel raccogliere informazioni personali può:

a) richiedere ad un soggetto di dati di fornire tali informazioni, a meno che

questo non sia richiesto per disposizione di legge, e di ciò l'individuo sia stato preventivamente informato;

b) richiedere ad un soggetto di dati di fornire volontariamente imformazioni personali, a meno di autorizzazione legale in merito, e di preventiva segnalazione all'individuo che la rivelazione delle informazioni è volontaria;

c) mettere a disposizione di organizzazioni o persone non specificatamente autorizzate qualsiasi studio od elemento statistico derivante da elaborazioni di informazioni personali, con mezzi elettronici o manuali.

3. Ogni organizzazione che mantiene un sistema informativo che dissemina rapporti statistici o risultati di ricerca basati su informazioni personali estratte dal sistema stesso, ma che non utilizza i dati personali identificanti il soggetto di dati per i suoi lavori, e che presenta dichiarazioni in tal senso al Ministero dell'interno, è esentata dagli obblighi di cui ai commi 1 e 2.

ART. 4.

1. Qualsiasi organizzazione che in atto raccoglie, mantiene, usa o dissemina informazioni personali, o che si propone di stabilire un sistema informativo per dati personali, deve:

a) notificare l'esistenza e il tipo di ciascun sistema esistente al Ministero dell'interno;

b) dare notizia dell'esistenza e del tipo di ciascun sistema esistente in comunicati annuali interni e di stampa nazionali e regionali, in modo da portare all'attenzione dei soggetti di dati ed a quella pubblica, l'esistenza delle informazioni raccolte;

c) in caso di nuovi sistemi o di sostanziali modifiche ai sistemi esistenti, dare pubblica notizia e notifica al Ministero dell'interno, non meno di tre mesi prima dell'inizio dell'attivazione o della

modifica dei sistemi informativi onde dare a tutti gli individui interessati una ragionevole opportunità di presentare eventuali osservazioni;

d) assicurarsi che la pubblica notizia e l'informazione al Ministero dell'interno specifichino quanto segue:

1) nome del sistema;

2) scopo generale del sistema;

3) categorie delle informazioni generali contenute e numero approssimato delle persone in merito alle quali le informazioni sono mantenute;

4) le norme generali e particolari di prevista applicazione per l'archiviazione dei dati, la durata di archiviazione e le norme di cancellazione;

5) le categorie delle fonti di informazione;

6) una descrizione dei modi e tipi di utilizzazione delle informazioni, incluse le categorie di utenti, e le relazioni organizzative fra di essi;

7) le procedure attraverso le quali un individuo può:

I) essere informato che è un soggetto di dati nel sistema;

II) accedere alle informazioni a lui relative inserite nel sistema;

III) contestare l'accuratezza, la completezza, la tempestività e la pertinenza dei dati a lui relativi inseriti nel sistema, e richiederne eventualmente la modifica o la cancellazione;

8) le procedure attraverso le quali un soggetto di dati potrà accedere ai sistemi informativi usati per statistica e per ricerca, onde sottoporli ad analisi personale;

9) l'indirizzo ed il recapito telefonico delle persone direttamente responsabili per il sistema informativo.

ART. 5.

1. Ogni organizzazione che mantenga nel suo sistema informativo informazioni personali deve:

a) informare ogni individuo cui è richiesto di fornire informazioni personali se è legalmente obbligato o se può rifiutarsi di fornire le informazioni richieste, ed anche di tutte le conseguenze, eventualmente note, in caso di fornitura, o non fornitura, delle informazioni richieste;

b) richiedere l'autorizzazione scritta di ciascun soggetto di dati per l'eventuale disseminazione di parte o tutte le informazioni fornite, ad altre organizzazioni o sistemi non aventi autorizzato regolare accesso al sistema, indicando l'uso per cui tale disseminazione è richiesta, e le conseguenze eventualmente note, per il soggetto di dati, della concessione o non concessione di tale autorizzazione;

c) garantire, previa richiesta ed appropriata identificazione, a ciascun soggetto di dati il diritto di esaminare, in forma a lui comprensibile:

1) tutte le informazioni personali a lui relative;

2) la natura delle fonti di informazione;

3) i nomi di coloro che ricevono le informazioni relative, sia per autorizzazione di regolare accesso, sia per autorizzazione ad accesso occasionale;

d) assicurare il rispetto delle condizioni minime circa le possibilità di verifica del soggetto di dati:

1) durante le ore di ufficio;

2) personalmente, se esso si presenta direttamente all'organo interessato e fornisce appropriata identificazione;

3) per posta, se ha presentato richiesta scritta con adeguate informazioni identificative;

e) assicurare che nessuna informazione personale relativa ad un soggetto di dati venga resa disponibile dal sistema, su richiesta di informazioni presentata attraverso un procedimento legale, senza che debito preavviso venga dato al soggetto di dati interessato alla richiesta di informazioni predetta;

f) seguire le sottoindicate procedure minime se il soggetto di dati informa che desidera correggere, chiarificare, o fare obiezioni circa le informazioni a lui relative, contenute nel sistema informativo:

1) l'organizzazione che mantiene il sistema informativo verifica e documenta lo stato corrente di tali informazioni;

2) se dopo le predette verifiche tali informazioni saranno riscontrate incomplete, non accurate, non pertinenti, non aggiornate, non necessarie, o se non possono sostanzialmente venire verificate, tali informazioni devono essere cancellate;

3) se l'investigazione non risolve il contrasto, il soggetto di dati può presentare una sua dichiarazione di contestazione scritta in cui formalizza la sua posizione;

4) quando viene presentata una dichiarazione di contestazione scritta, l'organizzazione che mantiene il sistema informativo deve inserire nel sistema nota attestante che le informazioni relative al particolare soggetto di dati sono oggetto di contestazione. Tale nota deve essere comunicata insieme alle relative informazioni in caso di qualsiasi utilizzazione di esse, all'interno dell'organizzazione o fuori di essa;

5) in caso di correzione o di cancellazione di una informazione, l'organizzazione che mantiene il sistema informativo in cui tale informazione era contenuta, dovrà informare della correzione o della cancellazione qualunque utente interno od esterno che abbia nel passato utilizzato tale informazione;

6) in caso di mancata risoluzione di un contrasto, l'organizzazione informa

prontamente e chiaramente il soggetto di dati del suo diritto di portare le sue richieste davanti al competente ufficio del Ministero dell'interno.

ART. 6.

1. Ciascuna organizzazione che raccoglie, mantiene, usa o dissemina informazioni personali, entro un anno dalla data di entrata in vigore della presente legge, ed entro sei mesi dalla data di messa in opera di un sistema informativo, se tale data è posteriore alla data di entrata in vigore della presente legge, notifica per iscritto a ciascun soggetto di dati al di lui ultimo indirizzo conosciuto, quanto segue:

a) natura delle informazioni personali contenute nei sistemi informativi ed uso previsto;

b) nome dell'organizzazione ed indirizzo dove il soggetto di dati può esaminare o ottenere copia delle informazioni personali a lui pertinenti.

ART. 7.

1. Le norme della presente legge non sono applicabili alle informazioni personali inserite in sistemi o banche dati che vengano istituite e mantenute da organizzazioni dello Stato, per scopi di sicurezza interna e di difesa militare.

ART. 8.

1. Un apposito ufficio del Ministero dell'interno agisce quale organo di controllo per l'applicazione della presente legge. A tale scopo tale ufficio:

a) pubblica un « Annuario dei sistemi informativi personali » in cui siano contenute le specifiche caratteristiche di ciascun sistema informativo personale attivato in Italia;

b) emana un dettagliato regolamento organizzativo e tecnico per l'applicazione della presente legge;

c) promuove le attività di ricerca necessarie per le applicazioni della presente legge;

d) assiste le organizzazioni nell'applicazione della presente legge;

e) verifica il rispetto della presente legge da parte delle organizzazioni, e procede all'attivazione delle procedure contro le organizzazioni responsabili di violazioni di essa;

f) conduce pubbliche riunioni, con la presenza dei rappresentanti di tutte le parti interessate, per l'esame di casi controversi circa l'applicazione della legge;

g) avanza motivate proposte al Ministro dell'interno circa esigenze di eventuali eccezioni od esenzioni dall'applicazione della presente legge diverse da quelle di cui alla lettera *f)*;

h) presenta al Ministro dell'interno un rapporto annuale delle proprie attività. Il Ministro dell'interno trasmette alle Camere il rapporto.

ART. 9.

1. Nessuna delle organizzazioni interessate alla presente legge può rivelare alcuna informazione personale, professionale, tecnica, commerciale di cui sia venuta a conoscenza, eccetto per quanto richiesto dall'applicazione della legge stessa.

2. Tutte le informazioni rivelate per l'applicazione della presente legge, devono essere considerate riservate da coloro che ne vengano a conoscenza per ragioni d'ufficio; essi pertanto non ne devono farne uso o rivelarne il contenuto salvo che nei casi previsti dalla presente legge.

ART. 10.

1. È punito con la multa da lire 200.000 a lire 2 milioni o con la reclu-

sione da 6 mesi ad un anno, chiunque, dolosamente o colposamente:

a) mantiene un sistema informativo senza notifica dello stesso al Ministero dell'interno;

b) fa circolare informazioni personali violando la presente legge;

c) richiede, usa o comunque acquisisce informazioni personali violando la presente legge.

ART. 11.

1. Ogni individuo od organizzazione, o dipendente di organizzazione, che violi le disposizioni della presente legge, e che con tale comportamento rechi danno a qualsiasi individuo, è tenuto a corrispondere a quest'ultimo una somma a titolo di:

a) indennizzo per il danno materiale effettivo subìto dall'individuo;

b) indennizzo per danni morali, ove sussistano;

c) rimborso spese per azione legale.