MARIO G. LOSANO

UN PROGETTO DI LEGGE SULLA PROTEZIONE DEI DATI PERSONALI

SOMMARIO

1. Perché un progetto di legge sulla riservatezza? — 2. Leggi e progetti di legge in Italia, in Europa e in altri paesi. — 3. I principi fondamentali di una legge sulla riservatezza. — 4. Trasparenza e riservatezza: un difficile equilibrio. — 5. I principi fondamentali della sicurezza dei dati. — 6. Tre caratteristiche del progetto di legge proposto. — 7. Il testo del progetto di legge sulla protezione dei dati personali.

1. Perché un progetto di legge sulla riservatezza?

Il progetto di legge qui pubblicato è il frutto di una mia iniziativa personale, nella quale ho potuto avvalermi della collaborazione veramente preziosa di Isa Fadda, dell'Ufficio legislativo del Consiglio regionale della Lombardia. Il progetto non tiene dunque conto degli inevitabili compromessi politici o della ricerca del consenso; esso propone le soluzioni che ritiene valide sul piano culturale e realizzabili sul piano pratico, con preciso riferimento alla realtà italiana.

Due ragioni mi inducono a pubblicare il risultato del nostro lavoro.

In primo luogo, sarebbe desiderabile dare maggiore concretezza ad un dibattito che — imperniato in Italia soprattutto sui grandi principi, in assenza d'una specifica legge — finisce spesso per non tenere conto delle conseguenze pratiche derivanti dall'applicazione di quei principi trasformati in legge. Nel progetto che segue, certe soluzioni potranno piacere o non piacere; tuttavia il fatto di averne scelta e sviluppata coerentemente una soltanto dovrebbe incanalare il dibattito verso critiche e controproposte concrete. È sperabile che la futura discussione sul progetto di legge italiano ne tragga qualche vantaggio.

* Con il cortese consenso della direzione di « Micromega » riproduciamo lo scritto del prof. M.G. Losano che vi era stato pubblicato, sul numero di febbraio 1987, con il titolo « Il *computer* di cristallo ».

In secondo luogo, il testo proposto — pur con tutti i limiti che gli derivano da un'elaborazione privata ed individuale — serve a dimostrare quale alto grado di coordinamento tra norme è indispensabile affinché la legge funzioni. Da questo punto di vista, le lacune stesse e le stesse soluzioni non accettate si possono interpretare come un contributo di questo progetto alla sistematicità di future leggi sulla riservatezza.

Per facilitare l'analisi critica del progetto raccoglierò nei prossimi paragrafi alcune informazioni generali sulla legislazione italiana e straniera, nonché sui principi cui si ispirano le leggi sulla *privacy*. La futura legge italiana dovrà tenerne conto per evitare l'isolamento del nostro paese nella trasmissione dei dati personali oltre frontiera: le leggi straniere vietano infatti di inviare dati personali a quegli Stati che non offrono protezione analoga a quella dello Stato d'origine. Il ritardo legislativo si trasforma così in un vincolo per l'effettiva sovranità del parlamento italiano.

Seguiranno poi gli argomenti addotti contro una legislazione sulla *privacy* e le critiche con cui vengono respinti. Nell'ultimo paragrafo, infine, riassumerò quelli che mi sembrano gli elementi più caratterizzanti del progetto.

2. Leggi e progetti di legge in Italia, in Europa e in altri paesi.

Nella Comunità economica europea, l'Italia e la Grecia non hanno ancora una legge sulla tutela dei dati personali. La Spagna e il Portogallo dispongono di norme costituzionali che sanciscono i diritti informatici del cittadino. Tutti gli altri Stati, infine, hanno emanato una specifica legge sulla *privacy*. La situazione internazionale è riassunta dalla tabella qui pubblicata.

Le principali leggi sulla protezione dei dati personali:

Austria - Legge 18 ottobre 1978, n. 565.

Canada - *Privacy Act*, 1982.

Danimarca - Legge 8 giugno 1978, n. 293, sui registri privati; legge 8 giugno 1978, n. 294, sui registri dell'amministrazione pubblica.

Francia - Legge 6 gennaio 1978, nn. 78-17.

Germania Federale - Legge 27 gennaio 1977.

Gran Bretagna - Legge 12 luglio 1984.

Islanda - Legge n. 63, 1981.

Israele - Legge 574 II-1981.

Italia - Legge 1° aprile 1981, n. 121: nuovo ordinamento dell'amministrazione della pubblica sicurezza.

LUSSEMBURGO - Legge 30 marzo 1979: identificazione numerica delle persone fisiche e giuridiche; legge 31 marzo 1979: uso dei dati nominativi nei sistemi informatici.

NORVEGIA - Legge 9 giugno 1978, n. 48.

PORTOGALLO - Costituzione del 2 aprile 1976, art. 35.

SPAGNA - Costituzione del 23 dicembre 1978, artt. 18 e 105.

STATI UNITI - Legge 26 ottobre 1970: obiettività dei dati per la concessione di crediti; legge 31 dicembre 1974: sulla *privacy*; legge 13 dicembre 1980: sulla *privacy*.

SVEZIA - Legge 11 maggio 1973, n. 289, modificata con legge 1° luglio 1982: raccolta dei dati.

SVIZZERA - Direttive del Consiglio federale sull'elaborazione dei dati negli enti federali, 16 marzo 1981.

UNGHERIA - Codice civile del 1977, art. 83; decreto del 27 gennaio 1981: sui centri di calcolo.

In Italia, pur non esistendo una specifica legge sulla protezione dei dati personali, sono tuttavia in vigore alcune norme che tutelano i diritti informatici del cittadino. Lo Statuto dei lavoratori (legge 20 maggio 1970, n. 300) vieta « di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore » (art. 8). Inoltre vieta l'uso « d'impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori » (art. 4). Entrambi gli articoli sono stati usati come strumenti per proteggere i dati personali dei lavoratori inclusi nelle banche di dati di un'impresa.

La legge sulla riforma della pubblica sicurezza (1° aprile 1981, n. 121) contiene negli articoli da 6 a 12 una vera e propria mini-legge sulla tutela dei dati personali elaborati dalla polizia. Va notato che queste norme offrono una tutela proprio nei campi in cui le leggi straniere tendono ad escludere l'applicazione delle leggi generali sulla *privacy*.

Una futura legge italiana dovrà tener conto di queste norme già esistenti, per evitare disposizioni contrastanti o inutili gravami a chi gestisce le banche di dati personali.

Alcune proposte di legge sono state presentate negli anni passati al parlamento italiano. Sono decaduti per la fine della legislatura il progetto Accame del 1981 e il progetto Picano del 1982. Dal 1984 sono pendenti il progetto Picano (ripresentato), il progetto Seppia e il progetto Martinazzoli, che riprende sostanzialmente il testo predisposto nel 1983 dalla commissione Mirabelli. Finora, tuttavia, essi sono stati esaminati soltanto dalla commissione Giustizia della Camera dei deputati, che ha iniziato a discuterne nell'ottobre 1986.

3. I PRINCIPI FONDAMENTALI DI UNA LEGGE SULLA RISERVATEZZA.

Ogni legge sulla riservatezza dei dati personali detta norme che si aggiungono a quelle già esistenti a tutela della riservatezza: per esempio, le norme sul segreto professionale o d'ufficio, ovvero il dovere di fedeltà all'impresa. Infatti, poiché l'informatica ha esteso la possibilità di ledere il diritto alla riservatezza, è necessario estendere la tutela accordata e superare i limiti tradizionali posti dalle norme pre-informatiche. Queste ultime, però, conservano il loro pieno vigore.

Compito d'una legge sulla riservatezza è non già di limitare la circolazione dei dati personali, bensì di renderne trasparente la circolazione evitando ogni abuso. Le sue norme devono quindi bilanciare e armonizzare la tutela dei diritti fondamentali dell'individuo con le esigenze di un'economia informatizzata e sovranazionale. Le soluzioni proposte sono quindi sempre soluzioni di compromesso; e il compromesso si fonda su una scelta politica, in cui si antepone la tutela di un bene a quella di un altro. In questo lavorio di bilanciamento, ogni situazione, ogni problema può trovare molteplici soluzioni giuridiche. L'importante è che l'insieme delle soluzioni scelte sia un insieme coerente.

Le leggi sulla riservatezza sono dunque testi complessi. L'intricata legge inglese del 1984, per facilitare l'orientamento del cittadino e dell'interprete, ha riassunto in otto punti i principi della protezione dei dati, includendoli in un allegato che costituisce parte integrante della legge stessa. Per fornire un primo quadro delle misure che devono essere contenute in una legge sulla riservatezza può essere utile riprodurli qui per esteso, nella traduzione pubblicata dal *Notiziario di informatica* della Camera dei deputati (1985, n. 1, p. 42).

« 1) Le informazioni componenti i dati personali devono essere acquisite e i dati personali devono essere elaborati secondo correttezza e secondo legge.

2) I dati personali possono essere conservati solo per uno o più scopi specifici e leciti.

3) I dati personali conservati per uno o più scopi non possono essere utilizzati o rivelati in modo incompatibile con lo scopo o gli scopi stessi.

4) I dati personali conservati per uno o più scopi devono essere adeguati, pertinenti e non sproporzionati rispetto allo scopo o agli scopi di cui sopra.

5) I dati personali devono essere accurati e, nei casi in cui sia necessario, mantenuti aggiornati.

6) I dati personali per uno o più scopi non possono essere conservati più a lungo di quanto sia necessario allo scopo o agli scopi stessi.

7) Ogni persona ha il diritto: *a*) ad intervalli ragionevoli e senza ritardi o spese ingiustificate: — di essere informata da un utente di dati se egli conservi o meno dati personali che la riguardano; — di avere

accesso a qualsiasi dato conservato da un utente di dati; *b*) se nel caso, di far correggere o cancellare tali dati.

8) Si devono adottare misure di sicurezza adeguate per impedire l'accesso non autorizzato, l'alterazione, la rivelazione o la distruzione di dati personali, come anche la perdita o la distruzione accidentale dei dati stessi ».

Una legge fondata su questi principi (o su principi analoghi) non costituisce un ostacolo alla circolazione delle informazioni, così come il codice stradale non costituisce un ostacolo alla circolazione automobilistica. Semplicemente, quando la circolazione ha superato una certa soglia, è indispensabile sottoporla a regole precise, affinché alcuni dei cittadini non subiscano svantaggi ingiustificati ed altri non ne traggano vantaggi altrettanto ingiustificati.

4. Trasparenza e riservatezza: un difficile equilibrio.

Nonostante le argomentazioni fin qui svolte, non mancano prese di posizione che dichiarano non necessaria una legge sulla riservatezza dei dati individuali. A favore di questa forma di *deregulation* si possono addurre tre argomenti. Dal punto di vista *economico*, le leggi sulla riservatezza impongono un onere alle imprese e agli enti che gestiscono banche di dati personali; quest'onere può essere ritenuto eccessivo rispetto al valore del bene da tutelare. Dal punto di vista *tecnico*, ci si chiede se le leggi sulla riservatezza — nate negli anni Settanta — siano ancora pienamente applicabili dopo la diffusione di sempre più potenti *personal computer*; questa diffusione può essere ritenuta incompatibile con un effettivo controllo sulle banche di dati. Dal punto di vista *politico*, infine, ci si chiede se le esigenze di controllo democratico non impongano il contrario della riservatezza, cioè la pubblicità, almeno in specifici campi: il dibattito svizzero sul segreto bancario ovvero le polemiche italiane sul segreto di Stato indicano che certi riserbi sono tanto più gelosi, quanto più turpi sono i traffici che essi celano. Un'ulteriore estensione della riservatezza può quindi essere ritenuta incompatibile con le esigenze di una società democratica.

Queste obiezioni non mi sembrano accettabili, anche se nel progetto di legge ho cercato di tenere conto di alcune giuste esigenze da esse espresse. Ecco in estrema sintesi le possibili risposte alle tre obiezioni appena esposte. Il costo della riservatezza è sopportabile se l'ente o l'impresa ha una gestione tecnicamente corretta del proprio centro di calcolo: su questo tema ritornerà il prossimo paragrafo. La diffusione dell'informatica individuale, grazie ai *personal computer*, impone forme semplificate di notifica e controllo, non già l'assenza di ogni regola e, quindi, la libertà di uso e di abuso dei dati personali. Infine, la trasparenza della gestione pubblica ed il controllo su di essa devono essere regolate da norme e da competenze precise. Su quest'ultimo punto è necessaria qualche precisazione.

Un ordinamento giuridico privo di norme che regolino l'accesso ai dati personali può reggere una società in cui le libertà individuali deperiscono: infatti, la legge sulla riservatezza stabilisce quali sono gli abusi, e li punisce; essa, da un lato, vieta la diffusione non autorizzata dei dati personali, ma, dall'altro, obbliga il detentore a renderli manifesti a chi ha il diritto di conoscerli. In Italia, oggi, non esiste né questo diritto, né quel dovere.

Una società post-industriale dove tutti accedono ai dati di tutti è un'utopia che si rivela irrealizzabile non appena questo principio generale viene applicato a casi concreti. Meglio allora una legge rigorosa che s'ispiri ai modelli scandinavi, secondo cui è vietato in linea di principio raccogliere dati personali, salvo i casi in cui ciò sia espressamente autorizzato.

Bisogna distinguere l'accesso ai dati personali dal più generale diritto del cittadino all'informazione. L'informazione del cittadino è uno strumento di controllo democratico che può fondarsi anche su dati non personali. Questo discorso riguarda i rapporti tra cittadino e istituzione, nonché le norme che li regolano: è questo un tema d'importanza capitale, ma diverso da quello della riservatezza.

Esso riguarda, ad esempio, l'attuazione dell'art. 25 della legge del 17 dicembre 1985, n. 816. Vi si legge che « tutti i cittadini hanno il diritto di prendere visione di tutti i provvedimenti adottati dai Comuni, dalle Province, dai Consigli circoscrizionali, dalle aziende speciali di enti territoriali, dalle Unità sanitarie locali, dalle Comunità montane ». Questa norma ed i relativi regolamenti di attuazione — in corso di emanazione presso i vari Comuni — portano però la discussione su un diritto diverso da quello della riservatezza; e non è possibile occuparcene ora.

Bisogna insomma non cedere alla tentazione cui spinge il disfacimento dell'apparato amministrativo italiano: quella di supplire alle carenze del sistema con un uso improprio di leggi esistenti. Come è inammissibile l'uso dello Statuto dei lavoratori come surrogato della legge sulla riservatezza dei dati personali, così è inammissibile l'uso di quest'ultima legge come surrogato della legge sull'informazione del cittadino.

La trasparenza dell'operare politico è compatibile con la tutela della riservatezza individuale; le due sono quindi non contrapposte, bensì complementari. Poiché non sono la stessa cosa, vanno regolate con norme diverse.

5. I PRINCIPI FONDAMENTALI DELLA SICUREZZA DEI DATI.

L'ultimo dei principi esposti al paragrafo 3 si riferisce alla sicurezza dei dati, cioè ai presupposti materiali necessari per proteggerli da interferenze indebite. Per ritornare al paragone automobilistico, non

basta stabilire che il furto è punito: è meglio chiudere a chiave l'auto e mettere l'antifurto; più in generale, a tutela dell'integrità fisica dei consociati, si stabilisce un controllo decennale sullo stato di funzionamento dell'auto. Lo stesso deve avvenire con l'informatica: è necessario non solo che l'indebito accesso ai dati personali venga punito, ma pure che esso venga il più possibile prevenuto con misure concrete che si riferiscano tanto ai programmi quanto all'organizzazione. Nelle leggi sulla *privacy*, le norme sulla sicurezza sono ricordate quasi sempre in un breve articolo o poco più. Infatti non è possibile stabilire in termini generali quali misure pratiche debba prendere il singolo centro per garantire, ad esempio, un'accettabile sicurezza dei propri locali. Eppure la normativa sulla sicurezza è una delle maggiori fonti di spesa per le imprese e per gli enti che debbono applicarla. Perciò, in questa premessa, ad essa viene dedicata un'attenzione pari a quella dedicata alle norme sulla tutela giuridica dei dati individuali. Ancora una volta, per concretezza, si richiama un testo legislativo già in vigore.

La legge federale tedesca del 1978 sintetizza in un decalogo le misure di sicurezza che devono essere adottate dai centri che elaborano dati personali. La traduzione è tratta dal volume *Banche dati e tutela della persona*, la cui seconda edizione è stata pubblicata dalla Camera dei deputati nel 1983:

« Se vengono elaborati in forma automatica dati personali, per l'esecuzione delle disposizioni della presente legge devono essere adottate misure idonee in relazione alla natura dei dati personali da tutelare:

1) impedire alle persone non autorizzate l'accesso agli impianti per l'elaborazione di dati con i quali vengono elaborati dati personali (controllo sull'accesso);

2) impedire che le persone che svolgono un'attività dell'elaborazione di dati personali asportino senza autorizzazione supporti di dati (controlli sull'asporto);

3) impedire l'inserimento non autorizzato nella memoria nonché la conoscenza, la modifica o la cancellazione di dati personali memorizzati (controlli sulla memoria);

4) impedire l'utilizzazione da parte di persone non autorizzate di sistemi di elaborazione dei dati dai quali o nei quali vengono trasmessi dati personali attraverso dispositivi autonomi (controllo di utilizzazione);

5) assicurare che le persone autorizzate ad utilizzare un sistema di elaborazione di dati attraverso dispositivi autonomi possano accedere esclusivamente ai dati personali per i quali sono stati autorizzati (controllo di disponibilità);

6) assicurare che possa essere successivamente controllato e accertato a quali uffici dati personali possano essere trasmessi attraverso dispositivi autonomi (controlli di trasmissione);

7) assicurare che possa essere successivamente controllato e accertato quali dati personali, in quale tempo, e da chi sono stati immessi in un sistema di elaborazione di dati (controlli di immissione);

8) assicurare che dati personali che vengono elaborati su incarico di altri possano essere elaborati soltanto conformemente alle istruzioni del committente (controlli sull'incarico);

9) assicurare che nella trasmissione di dati personali, nonché nel trasporto dei corrispondenti supporti di dati, questi non possano essere letti, modificati o cancellati (controlli sul trasporto);

10) impostare l'organizzazione aziendale interna o esterna in modo tale che sia adeguata alle particolari esigenze della protezione dei dati (controlli di organizzazione) ».

La riprova del fatto che le leggi sulla protezione dei dati non impongono oneri eccessivi alle imprese è data dal fatto che queste misure di sicurezza sono, in generale, già adottate dalle grandi aziende per tutelare i propri dati anche non personali, ma di ricerca, di contabilità, di *marketing* eccetera. Sono adottate, si noti, indipendentemente dall'esistenza di una legge sulla protezione dei dati personali. Non si può dire lo stesso, invece, per le piccole e medie imprese. Dato lo sviluppo dell'informatica in questi ultimi anni, è necessario che queste regole vengano fissate in termini generali, in modo che la tutela dei dati del singolo individuo non dipenda più dalla buona volontà della singola impresa. Il diritto alla riservatezza è un diritto fondamentale e deve quindi esere garantito per tutti in egual misura.

6. Tre caratteristiche del progetto di legge proposto.

Ogni legge sulla protezione dei dati costituisce un compromesso sulla tutela di beni spesso in concorrenza tra loro. Questo compromesso va raggiunto non sulla base di bilanciamenti tanto nobili quanto astratti sui diritti e doveri del cittadino, bensì in concreto, tenendo conto della realtà sociale e politica dello Stato in cui la legge dovrà essere applicata. Per questo il progetto che segue prende posizione su alcune grandi scelte che si impongono in ogni legge sulla *privacy* e vi aggiunge alcune caratteristiche legate alla specificità dell'Italia. La tutela della legge viene riconosciuta alle persone fisiche, ma non a quelle giuridiche; le norme si applicano tanto alle banche di dati quanto agli schedari manuali o simili; gli organi previsti dalla legge si ispirano a quelli già esistenti negli Stati membri della CEE, ma tengono conto che i diritti fondamentali, in Italia, vanno tutelati attraverso la magistratura ordinaria.

Senza voler commentare i singoli articoli, vanno illustrate almeno tre proposte contenute nel progetto.

a) Il decentramento regionale. La struttura dello Stato italiano si situa a metà strada fra il centralismo francese e il federalismo tedesco. Il progetto tiene conto della realtà regionale prevedendo organi tanto centrali quanto regionali nell'applicazione delle norme. Questa soluzione fa propria l'esperienza tedesca (che proprio su questa

legge conobbe forti tensioni tra Bund e Länder) e nel contempo propone una struttura organizzativa più veloce nel decidere i singoli casi.

b) *L'intervento per gruppi di lavoro.* Sempre al fine di rendere più spedita la decisione dei programmi sottoposti alle autorità di controllo, il progetto propone che queste agiscano mediante gruppi di lavoro (*task forces*) che si formano su ciascun problema e si sciolgono al compimento del lavoro. Questa soluzione permette di raggruppare di volta in volta le competenze specifiche richieste dal caso singolo, che può esigere conoscenze specialistiche molto approfondite. Inoltre limita il formarsi di una burocrazia informatica, troppo facilmente esposta a pressioni d'ogni genere. Il principio di formare e di sciogliere gruppi di lavoro in funzione del singolo caso è prassi costante, ad esempio, nell'organizzazione della revisione interna (*audit*) delle grandi imprese.

c) *Il problema delle sanzioni.* Le sanzioni proposte dal progetto sono gravi sia per il cittadino che viola le norme, sia per il funzionario che viene meno ai suoi doveri.

La discussione sulle sanzioni è d'importanza decisiva per la reale rilevanza della legge, ma si scontra con problemi di difficile soluzione. Ad esempio, l'ordinamento giudiziario italiano ha ritmi di lavoro incompatibili con la gestione dei centri di calcolo e, inoltre, prevede istituti come il patteggiamento che possono svuotare la sanzione proposta. Non si dimentichi che i reati contro la riservatezza sono *white collar crimes*, commessi per lo più da persone incensurate e di livello sociale medio-alto: insomma, si può essere quasi certi che i giudici tenderanno ad applicare il minimo delle pene.

D'altra parte, le sanzioni troppo gravi portano alla disapplicazione della legge, mentre quelle troppo lievi la rendono inutile. Per questo, nei casi più gravi, è indispensabile che la pena detentiva si cumuli con quella pecuniaria, e non che sia ad essa alternativa. Nei casi di minor gravità la pena pecuniaria deve avere un peso rilevante: si può giungere a questo fine stabilendo che essa venga applicata per ogni singola violazione, ovvero fissandone il valore come percentuale di un parametro del reddito individuale o aziendale.

Le sanzioni applicate ai funzionari infedeli o inetti sono indispensabili al funzionamento della legge. Infatti l'impresa o l'ente che apre i suoi archivi all'organo di controllo deve poter difendersi dall'eventuale propagazione di suoi dati riservati; in caso contrario negherà la propria cooperazione.

I termini entro cui deve muoversi l'autorità di controllo sono termini perentori e sanzionati; in caso contrario, i tempi della procedura divengono incompatibili con le esigenze della gestione d'un centro di calcolo, imponendo un danno o al singolo o all'impresa.

Indipendentemente dalla soluzione concreta accettata, la reale applicazione d'una legge sulla protezione dei dati personali dipende

dalla rapidità con cui si giunge alla decisione della controversia e dall'effettiva temibilità delle sanzioni.

In assenza di queste due condizioni, la futura normativa italiana sulla riservatezza dei dati individuali avrà il vantaggio d'impedire l'esclusione dell'Italia dal flusso transnazionale dei dati, ma non sarà in grado di offrire una tutela reale (cioè al passo coi tempi) per uno dei diritti fondamentali dell'individuo.

PROGETTO DI LEGGE SULLA PROTEZIONE DEI DATI PERSONALI

TITOLO PRIMO
Disposizioni generali

Articolo 1.
Criteri generali di applicazione.

1) La formazione e gestione di banche di dati personali, gestite su elaboratore o manualmente, è consentita secondo le modalità della presente legge e con il consenso dell'interessato, al fine di evitare ogni lesione ai diritti e alla libertà dell'individuo, costituzionalmente garantiti.

2) Alla tutela dei diritti informatici delle persone fisiche sono preposti organi statali e regionali, istituiti dalla presente legge e denominati garanti pubblici.

Articolo 2.
Definizioni dei termini informatici.

1) Ai fini della presente legge i termini informatici sono definiti nei commi seguenti:

2) Per « dati personali » si intendono i dati riferiti o riferibili ad una persona fisica individualmente identificabile; non ricadono sotto la protezione della presente legge i dati personali anagrafici raccolti dai Comuni e quelli relativi a nome, cognome e indirizzo raccolti da privati.

3) Per « banca di dati » si intende un insieme di dati personali raccolti secondo criteri predeterminati e reperibili secondo criteri diversi, indipendentemente dal procedimento tecnico usato.

4) Per « memorizzazione » del dato personale si intende la sua registrazione su un supporto che ne consenta la conservazione e il trattamento secondo i criteri indicati al comma 2 del presente articolo, indipendentemente dal procedimento tecnico usato.

5) Per « accesso » al dato si intende il renderlo accessibile al titolare del dato stesso.

6) Per « comunicazione » del dato personale si intende il renderlo accessibile a terzi diversi sia dal titolare del dato, sia dal soggetto obbligato, definito all'art. 3.

7) Per « modificazione » del dato personale si intende qualsiasi mutamento di una parte del dato originario.

8) Per « blocco » del dato personale si intende la pura conservazione del dato:

a) con riferimento ad un suo uso concluso; *b*) in attesa di accertamenti e decisioni su dati contestati; in entrambi i casi il blocco esclude la possibilità di ulteriori elaborazioni.

9) Per « cancellazione » del dato personale si intende il rendere inaccessibile il dato stesso.

Articolo 3.
Soggetti obbligati.

1) Salvo esplicite eccezioni stabilite dalla legge, le presenti disposizioni si applicano:

a) a tutti gli organi, organismi e uffici della pubblica amministrazione centrale e periferica, nonché degli enti locali, che elaborano dati personali;

b) alle persone giuridiche, anche non riconosciute, che elaborano dati per finalità proprie;

c) alle persone giuridiche, anche non riconosciute, che elaborino dati per conto altrui;

d) alle persone fisiche che elaborano dati personali per fini secondo le modalità stabilite all'art. 43.

2) Ai fini della presente legge, i soggetti di cui alle precedenti lett. *a*), *b*) e *c*) sono denominati « soggetti obbligati ».

Articolo 4.
Segreto d'ufficio.

1) I dati di cui gli organi e gli uffici competenti ai sensi della presente legge vengano a conoscenza nello svolgimento delle loro funzioni sono coperti dal segreto d'ufficio.

2) La violazione di questo dovere comporta le aggravanti previste dall'art. 50 di questa legge.

Articolo 5.
Sicurezza degli impianti.

1) Il soggetto obbligato deve impedire che, in modo illegittimo, sia possibile accedere ai dati personali, modificarli o comunicarli a terzi; e che, in modo accidentale, essi possano andar perduti in tutto o in parte.

2) Il soggetto obbligato è perciò tenuto a garantire:

— la sicurezza fisica del luogo dove i dati vengono conservati ed elaborati;

— la sicurezza fisica e logica della strumentazione informatica e di quella ad essa complementare;

— l'affidabilità del personale che ha accesso ai dati ed ai locali dove essi vengono conservati o elaborati.

3) Nel valutare le misure di sicurezza si tiene conto che il loro costo deve essere proporzionato alla finalità di protezione che esse si prefiggono.

Titolo Secondo
Diritti informatici soggettivi della persona fisica

Articolo 6.
Diritto all'informazione.

1) Ogni persona fisica ha il diritto di essere preventivamente informata della memorizzazione di ogni suo dato personale, sulla quale deve fornire il proprio consenso scritto.

Articolo 7.
Diritto di accesso.

1) Ogni persona fisica ha diritto di accedere all'insieme dei dati personali che la riguardano, secondo le procedure previste dal Titolo terzo della presente legge.

Articolo 8.
Diritto di intervento sul dato.

1) Ogni persona fisica ha il diritto di far rettificare i dati personali che gli risultino errati.

2) Qualora il dato risulti incompleto, l'interessato ha il diritto di chiederne le necessarie modifiche o la cancellazione.

3) Qualora i presupposti del consenso siano venuti meno l'interessato può concordare col soggetto obbligato:

a) il blocco dei propri dati, per evitarne l'utilizzazione a fini diversi da quelli originari;

b) la cancellazione, qualora il soggetto obbligato riconosca che ciò non gli arreca pregiudizio.

Articolo 9.
Diritto di reclamo.

1) Qualora l'esercizio dei diritti di cui al presente titolo venga precluso o limitato, l'interessato può adire i garanti pubblici:

a) per far dirimere la controversia;

b) per far controllare l'esecuzione tecnica dell'accordo di cui all'art. 8, comma 3, in relazione all'intervento sul dato personale.

Articolo 10.
Partecipazione.

1) Le persone fisiche, sia individualmente, sia organizzate, possono sottoporre ai garanti pubblici proposte per modificare la presente legge e adeguarne l'applicazione.

2) In relazione ai risultati dell'attività svolta ed alle osservazioni ricevute, i garanti pubblici sottopongono all'esame degli organi competenti l'aggiornamento delle disposizioni della presente legge.

Titolo Terzo
Obblighi dei titolari delle banche di dati personali.

Articolo 11.
Obbligo di richiesta di consenso.

1) I titolari delle banche di dati personali, prima di procedere alla raccolta e alla memorizzazione di dati personali, devono chiedere ed ottenere in forma scritta il consenso del diretto interessato.

2) È fatto divieto di utilizzare i dati personali così raccolti per finalità diverse da quelle per cui si è ottenuto il consenso.

3) I dati personali memorizzati non possono essere comunicati a terzi, salvo il consenso scritto del titolare dei dati e salve esplicite deroghe previste per legge.

4) Qualora la memorizzazione di dati personali venga effettuata per conto di terzi, i dati stessi possono essere trasmessi soltanto al soggetto per conto del quale sono stati raccolti ed elaborati.

Articolo 12.
Obbligo di notifica delle banche di dati personali.

1) Chi intende realizzare una banca di dati personali deve darne notizia al garante competente di cui all'art. 18, nonché al responsabile per la protezione dei dati personali di cui all'art. 14, entro i termini e secondo le modalità stabilite dagli organi competenti ai sensi della presente legge.

2) L'elenco dei dati contenuti nella notifica è tassativo. Pertanto la variazione di ogni elemento elencato nel seguente art. 13 va notificata al competente garante nel termine perentorio di 15 giorni dal momento del suo verificarsi.

3) La registrazione ha effetto per tre anni. Alla sua scadenza va rinnovata anche se non vi sono mutamenti nei dati notificati. Il soggetto obbligato può chiedere registrazione e rinnovi per periodi più brevi, ma comunque non inferiori ad un anno.

4) Il regime economico della registrazione e dei rinnovi è regolato dall'art. 54, commi 1 e 2.

Articolo 13.
Contenuto minimo della notificazione.

1) Costituiscono il contenuto minimo della notificazione d'una banca di dati — e quindi del registro dei garanti e del responsabile dei dati — almeno i seguenti elementi:

— nome o ragione sociale e indirizzo del soggetto obbligato;

— oggetto dell'attività e settore merceologico del soggetto obbligato;

— strumenti usati nella gestione delle banche di dati;

— descrizione per ogni singola banca di dati della natura dei dati personali memorizzati e della o delle finalità per cui essi sono memorizzati;

— fonti attuali o potenziali dei dati;
— destinatari attuali o potenziali delle comunicazioni di quei dati, aventi sede legale o residenza in Italia;
— destinatari attuali o potenziali della comunicazione di quei dati, aventi sede legale o residenza all'estero;
— indirizzo del responsabile che garantisce l'accesso ai dati.

Articolo 14.
Nomina del responsabile per la protezione dei dati personali.

1) I soggetti obbligati sono tenuti a nominare, previo parere delle organizzazioni sindacali interne, il responsabile per la protezione dei dati personali.
2) Ad esso si rivolgono gli interessati, al fine di esercitare i diritti informatici di cui al precedente Titolo secondo, ed i garanti pubblici nello svolgimento dei loro compiti di indagine e controllo.
3) Il responsabile delle banche di dati personali:
a) dev'essere in possesso di comprovata esperienza organizzativa, informatica e giuridica;
b) dev'essere posto alle dirette dipendenze del vertice della direzione aziendale, ovvero, nelle pubbliche amministrazioni e negli enti di diritto pubblico, dei rispettivi organi esecutivi.
4) In relazione alle dimensioni delle banche di dati personali, l'incarico di responsabile può cumularsi con altre mansioni gestionali o d'istituto, purché ciò non pregiudichi l'adempimento dei compiti attribuitigli nell'ambito della protezione dei dati personali.

Articolo 15.
Compiti del responsabile per la protezione dei dati personali.

1) Al responsabile dei dati personali sono attribuite le seguenti funzioni:
a) la predisposizione della normativa interna necessaria a garantire il puntuale adempimento della presente legge, nonché il controllo formale sulla sua applicazione;
b) l'istituzione, la gestione e l'aggiornamento del registro delle banche di dati personali attivate presso il soggetto obbligato;
c) la comunicazione delle informazioni necessarie rispettivamente agli interessati per esercitare i propri diritti informatici, e ai garanti pubblici per esercitare i propri compiti;
d) le osservazioni ed i suggerimenti, rivolti sia alla direzione aziendale, sia ai garanti pubblici, al fine di modificare la presente legge e di adeguarne l'applicazione.

Articolo 16.
Responsabilità.

1) Dei compiti di cui al precedente art. 15 risponde in proprio il responsabile dei dati personali; non gli sono però imputabili le violazioni materiali alla normativa interna, non rilevabili attraverso il controllo formale di sua competenza.

Titolo Quarto
I garanti pubblici

Articolo 17.
Il garante nazionale e i garanti regionali.

1) Gli organi preposti alla tutela dei diritti informatici soggettivi sono i garanti pubblici operanti a livello nazionale e regionale, secondo le disposizioni del presente titolo.
2) I garanti devono essere scelti tra persone di comprovata esperienza organizzativa, informatica e giuridica e di riconosciuta autorità morale, in modo da garantire la massima indipendenza ed obiettività di giudizio.
3) I garanti nazionali e regionali restano in carica cinque anni. Non sono confermabili e, alla scadenza del mandato, rimangono in carica fino all'insediamento dei successori.

Articolo 18.

Competenze dei garanti pubblici.

1) È istituito il garante pubblico nazionale, che ha competenza per la protezione dei dati personali, relativa alle banche di dati di:

a) ogni ufficio dell'amministrazione statale, anche a gestione autonoma, sia centrale, sia periferica;

b) enti pubblici, anche economici, con sede sociale in Roma;

c) banche di interesse nazionale.

2) In ogni Regione a statuto ordinario o speciale è istituito il garante pubblico regionale, che ha competenza per la protezione dei dati personali relativa alle banche di dati di:

a) ogni ufficio dell'amministrazione regionale, anche a gestione autonoma, ed anche a livelli decentrati;

b) Province, Comuni, enti locali singoli o associati;

c) enti pubblici o privati con sede legale nel territorio della Regione;

d) ogni altro soggetto obbligato non previsto nelle competenze del garante nazionale.

Articolo 19.

Nomina del garante nazionale.

1) Il garante nazionale è nominato dal presidente del Senato e da quello della Camera dei deputati, d'intesa tra loro, e ha sede presso la Camera dei deputati.

Articolo 20.

La Commissione Informatica Nazionale.

1) È istituita una commissione bicamerale per la protezione dei dati personali, denominata « Commissione Informatica Nazionale » e composta da parlamentari ed esperti esterni, per un totale di 9 membri per ciascun ramo del parlamento.

2) Le commissioni Affari costituzionali del Senato e della Camera dei deputati propongono alle rispettive assemblee una lista di candidati, aventi i requisiti di cui al precedente art. 17, comma 2, nell'ambito delle quali vengono eletti i componenti della Commissione Informatica Nazionale.

3) La Commissione è presieduta dal garante nazionale.

Articolo 21.

Nomina dei garanti regionali.

1) Il garante regionale è eletto dai Consigli regionali con la maggioranza dei due terzi dei consiglieri assegnati alla Regione.

2) Nel caso in cui nessuno dei candidati ottenga tale maggioranza nelle prime tre votazioni, la nomina è effettuata dal Consiglio regionale nella seduta successiva ed è valida se il candidato abbia ottenuto la maggioranza assoluta dei voti.

3) Il garante regionale ha sede presso i Consigli regionali.

Articolo 22.

La Commissione regionale per la protezione dei dati personali.

1) Ciascun consiglio regionale istituisce, ai sensi del proprio regolamento interno, la Commissione speciale per la protezione dei dati personali, composta da consiglieri regionali ed esperti in pari numero, aventi i requisiti di cui al precedente art. 17, comma 2.

2) La commissione è presieduta dal garante regionale per la protezione dei dati personali.

Articolo 23.

Compiti delle Commissioni nazionale e regionale per la protezione dei dati personali.

1) Le Commissioni per la protezione dei dati personali sono lo strumento operativo collegiale per l'applicazione della presente legge.

2) In particolare ad esse sono attribuite le seguenti funzioni:

a) approvare le disposizioni cui debbono attenersi i soggetti obbligati per garantire la tutela dei diritti informatici;

b) controllare l'applicazione formale da parte dei soggetti obbligati delle disposizioni emanate dal garante;

c) istituire, gestire e aggiornare il registro delle banche di dati personali, attivate presso i soggetti obbligati, ricadenti nell'ambito della propria competenza;

d) deliberare la composizione dei gruppi di lavoro di cui al successivo art. 25, comma 1;

e) esaminare i giudizi dei gruppi di lavoro nei casi in cui il garante decida di investirne la Commissione.

Articolo 24.

Compiti dei garanti pubblici.

1) I garanti pubblici sovrintendono al funzionamento delle rispettive Commissioni, le convocano, ne predispongono l'ordine del giorno e firmano gli atti a rilevanza esterna.

2) Ai garanti pubblici sono attribuite in particolare le seguenti funzioni:

a) ordinare ai soggetti obbligati l'applicazione della normativa approvata dalla Commissione per la protezione dei dati;

b) stabilire i criteri per i controlli d'ufficio, i relativi tempi di realizzazione e le modalità organizzative della loro esecuzione;

c) pubblicare, entro il 31 dicembre di ogni anno, il registro aggiornato delle banche dei dati personali notificate presso la Commissione, curandone la distribuzione nelle forme ritenute più idonee a consentire l'accesso alle informazioni necessarie alla tutela ottimale dei diritti informatici;

d) comunicare le informazioni necessarie all'esercizio dei diritti informatici;

e) ricevere i reclami degli interessati che ritengano leso un proprio diritto costituzionalmente garantito a causa della memorizzazione di dati personali; metterli all'ordine del giorno della Commissione al fine di costituire, ove necessario, il gruppo di lavoro che esamina la doglianza;

f) comunicare alle parti il giudizio del gruppo di lavoro o della commissione plenaria.

Articolo 25.

Modalità operative delle Commissioni per la protezione dei dati personali.

1) In relazione alle questioni di volta in volta iscritte all'ordine del giorno delle sedute, le Commissioni formano gruppi di lavoro cui partecipano, ove necessario, anche esperti esterni iscritti all'albo di cui al successivo art. 31, comma 1.

2) Il giudizio del gruppo di lavoro viene trasmesso al garante, il quale decide se comunicarlo direttamente alle parti, ovvero sottoporlo all'esame della Commissione in seduta plenaria.

3) Il gruppo di lavoro si scioglie al momento della notifica del proprio giudizio alle parti, ovvero, nel caso di remissione alla Commissione, al momento in cui il garante notifica alle parti il giudizio della Commissione.

Articolo 26.

Diritti e doveri dei garanti.

1) Le funzioni di garante nazionale e regionale sono incompatibili con l'esercizio di qualsiasi altra attività lavorativa.

2) I garanti hanno l'obbligo del tempo pieno e della residenza nella capitale o nel capoluogo di regione, o comunque nella città sede del Consiglio regionale.

3) Ai garanti spetta il mantenimento del posto di lavoro nell'ente o impresa di provenienza per l'intera durata del mandato, senza sospensione della progressione di carriera per anzianità.

4) Il trattamento economico del garante nazionale e di quelli regionali è pari a quello previsto rispettivamente per i deputati e per i consiglieri regionali.

Articolo 27.

Relazione annuale.

1) Ogni garante è tenuto, a pena di decadenza, a pubblicare entro il 31 marzo di ogni anno una relazione riguardante l'anno solare precedente.

2) La relazione deve contenere in particolare:

a) l'analitica descrizione dell'attività svolta;

b) la descrizione della situazione del personale, delle macchine e attrezzature — anche di tipo non informatico — comunque disponibili, dei locali e dei finanziamenti;

c) la dettagliata valutazione circa l'adeguatezza della normativa ai casi sottoposti al suo esame;

d) specifiche indicazioni degli ostacoli incontrati nell'esercizio delle attività di istituto;

e) le proposte e osservazioni ricevute ai fini del miglioramento della legge;

f) i dati statistici richiesti dal regolamento di cui all'art. 31;

g) ogni altro elemento o questione che il garante ritenga utile sottoporre alla pubblica attenzione.

Articolo 28.
Informazione dei cittadini.

1) I garanti pubblici, nell'esercizio della loro attività, sono tenuti a creare le strutture organizzative e la documentazione atte a diffondere — soprattutto in forma divulgativa e semplificata — la conoscenza della presente legge e le modalità per l'esercizio dei diritti informatici, nonché le problematiche ad essi connesse.

Articolo 29.
Conferenza dei garanti.

1) Il presidente del Senato e della Camera dei deputati, d'intesa tra loro, convocano una conferenza annuale dei garanti, da tenersi entro il mese di giugno di ogni anno, per verificare l'omogeneità dei criteri di applicazione della presente legge e per sottoporre a una pubblica discussione le relazioni presentate dai garanti.

2) Detta conferenza è aperta alla partecipazione delle associazioni scientifiche, tecniche e professionali interessate all'informatica, nonché ai rappresentanti delle organizzazioni dei lavoratori e degli imprenditori.

Titolo Quinto
Le strutture organizzative dei garanti pubblici

Articolo 30.
Personale e strutture organizzative.

1) Presso i garanti pubblici sono istituite le strutture organizzative preposte all'applicazione della presente legge.

2) Il personale che vi è addetto può essere assunto per concorso pubblico, ovvero può essere scelto tra i funzionari pubblici già in servizio, utilizzando anche l'istituto del comando. In caso di documentata necessità può essere assunto a tempo determinato, previo avviso pubblico sui maggiori quotidiani, nel quale siano indicati i requisiti di esperienza, i titoli richiesti e le modalità di selezione.

Articolo 31.
Regolamento di esecuzione.

1) Con successivo regolamento, da emanarsi entro sei mesi dalla data di entrata in vigore della presente legge, il Ministero di Grazia e Giustizia disciplina con normative specifiche:

— le piante organiche del personale dei singoli garanti pubblici;

— le qualifiche professionali;

— l'organizzazione degli uffici, anche in relazione a quanto previsto dall'art. 24;

— le infrastrutture informatiche necessarie, nella loro configurazione minima;

— i criteri per la formazione e l'aggiornamento dell'albo degli esperti esterni, previsto dall'art. 25;

— il trattamento economico del personale;

— i criteri per la rilevazione ed elaborazione dei dati statistici connessi all'attività dei garanti, al fine di ottenere statistiche omogenee per l'intero territorio nazionale;

— ogni altro elemento necessario a garantire la massima funzionalità e tempestività nell'esercizio delle funzioni d'istituto, anche per il conseguimento di un rapporto ottimale tra garanti e cittadini.

Articolo 32.
Istituzione degli uffici.

1) Sulla base del regolamento di cui al precedente articolo, entro 3 mesi dalla sua emanazione, la Camera dei deputati e i Consigli regionali, nell'ambito delle rispettive competenze, istituiscono gli uffici e le strutture informatiche necessarie.

Articolo 33.
Procedimento di formazione del regolamento.

1) Il Ministero dell'Interno, entro tre mesi dalla data di entrata in vigore della presente legge, sulla base dei dati in suo possesso in base alle notifiche ricevute ai sensi della legge 1° aprile 1981, n. 121, è tenuto a fornire al Ministero di Grazia e Giustizia e ai Consigli regionali, in relazione alle competenze di cui all'art. 18, i dati conoscitivi sul numero e sulla consistenza delle banche di dati personali esistenti, articolati regione per regione.

2) I Consigli regionali, entro un mese dal ricevimento dei dati conoscitivi, possono esprimere il proprio parere al Ministero di Grazia e Giustizia circa la rispondenza alla reale situazione regionale dei dati forniti dal Ministero dell'Interno.

3) I Consigli regionali, devono essere consultati dal Ministero di Grazia e Giustizia sul contenuto del regolamento di cui al presente articolo, prima della sua approvazione.

TITOLO SESTO
Tutela dei diritti informatici

Articolo 34.
Istanze del cittadino.

1) Ogni persona fisica che ritenga lesi i propri diritti informatici, ovvero necessiti di informazioni atte ad accertare un'eventuale lesione, può fare istanza scritta, alternativamente, al responsabile aziendale per la protezione dei dati personali, ovvero ai garanti pubblici.

2) Il responsabile aziendale o il garante pubblico, che ha ricevuto la richiesta, è tenuto a rispondere entro 15 giorni dal suo ricevimento.

3) Nella risposta deve essere indicato il motivo per cui l'istanza è respinta, ovvero l'accoglimento della stessa e, nel caso di istanza rivolta al garante, la comunicazione dell'inizio delle procedure di cui all'art. 37.

4) Nel caso sia competente un garante o un responsabile aziendale diverso da quello adito, quest'ultimo trasmette l'istanza al soggetto competente e contemporaneamente ne informa l'interessato.

5) I termini di cui al presente articolo decorrono dalla data del timbro postale di arrivo della lettera raccomandata ovvero dalla data di protocollo dell'istanza presentata a mano.

Articolo 35.
Contenuto dell'istanza.

1) L'istanza deve contenere almeno i seguenti elementi:

— generalità e dati anagrafici dell'istante, nonché eventuale domicilio eletto ai fini della notifica della risposta;

— generalità o ragione sociale del titolare della banca di dati oggetto dell'istanza;

— sintetica descrizione della richiesta o della doglianza, integrata dalla documentazione in possesso dell'istante.

2) In assenza degli elementi di cui sopra, l'istanza viene dichiarata irricevibile e, entro il termine di cui al precedente art. 34, comma 2, viene restituita all'interessato per le opportune integrazioni.

Articolo 36.
Funzioni del garante.

1) Qualora l'istante si sia rivolto al responsabile dei dati personali e non abbia in quella sede ottenuto l'informazione richiesta, ovvero la rettifica del dato in contestazione, o non abbia raggiunto l'accordo sulla modalità dell'uso o della memorizzazione del dato personale, può ricorrere con reclamo al garante pubblico, ai sensi del precedente art. 9, per la tutela dei propri diritti informatici.

2) Qualora l'istante si sia rivolto direttamente al garante pubblico, questi assume le informazioni dal responsabile aziendale e le trasmette all'interessato nel termine di trenta giorni dal ricevimento dell'istanza.

Articolo 37.
Istruttoria e decisione.

1) Ricevuta l'istanza o il reclamo, il garante provvede ad affidarlo a personale del proprio ufficio, eventualmente integrato da esperti iscritti all'albo di cui all'art. 31, comma 1, formando di volta in volta gruppi di lavoro specializzati, in relazione alla specificità del caso in esame.

2) Esaurita l'istruttoria, il gruppo di lavoro redige una relazione che viene sottoposta all'esame della competente Commissione per la protezione dei dati personali, la quale decide a maggioranza dei presenti.

3) Il garante:

— firma la decisione, che viene notificata all'interessato;

— valuta l'esistenza degli estremi per un'eventuale sanzione amministrativa;

— segnala al cittadino la possibilità di adire il giudice civile per il risarcimento del danno;

— ha l'obbligo di rapporto all'autorità giudiziaria, qualora ravvisi una lesione del diritto informatico penalmente sanzionabile.

Articolo 38.
Rapporti tra garante e responsabile per la protezione dei dati personali.

1) Il garante — ovvero un membro scelto al proprio interno dalla Commissione per la protezione dei dati personali o un funzionario dell'ufficio del garante, da quest'ultimo espressamente delegato — ha diritto di accesso all'intera documentazione informatica relativa al soggetto che ha richiesto il suo intervento, anche se questi dati sono distribuiti fra più banche od archivi.

2) Il diritto di accesso comprende anche i documenti cartacei su cui si è direttamente fondata la memorizzazione.

3) Qualora per la completezza delle indagini si rendesse necessaria l'acquisizione di documenti cartacei precedenti a quello da cui si è direttamente desunto il dato originario e qualora il responsabile per la protezione dei dati personali opponesse all'accesso del garante o del suo delegato motivi di segreto industriale o di riservatezza, il garante stesso può adire il giudice ordinario, affinché assuma i provvedimenti necessari a rendere accessibile la documentazione richiesta, eventualmente depurata delle parti riservate irrilevanti ai fini dell'indagine.

Articolo 39.
Interventi d'ufficio del garante.

1) Il garante può espletare indagini a campione, per verificare che singole banche di dati abbiano ottemperato agli obblighi di cui al precedente Titolo terzo.

2) Qualora nello svolgimento dell'attività richiesta dal cittadino il garante, indipendentemente dalla doglianza presentata, accerti violazioni alle disposizioni della presente legge, ne dà notizia agli interessati per consentire loro le iniziative a tutela dei propri diritti, ovvero all'autorità giudiziaria, qualora riscontri violazioni penalmente sanzionabili.

Titolo Settimo
Comunicazione e trasmissione dei dati personali

Articolo 40.
Comunicazione dei dati di enti pubblici.

1) La comunicazione di dati personali tra uffici pubblici è consentita quando essa serva all'adempimento delle funzioni pubbliche di competenza dell'ufficio trasmittente o ricevente.

2) Le informazioni soggette al segreto professionale o d'ufficio possono essere comunicate esclusivamente ad uffici che perseguano finalità uguali a quelle dell'ufficio che ha raccolto i dati.

3) La comunicazione di dati personali memorizzati da uffici pubblici verso soggetti privati è consentita se il richiedente dimostra di essere titolare di un legittimo interesse a conoscerli, sem-

pre che ciò non costituisca un pregiudizio per il soggetto interessato.

4) L'ufficio pubblico comunicante è obbligato in ogni caso a informare contestualmente anche il soggetto interessato.

Articolo 41.
Flusso transnazionale dei dati personali.

1) È fatto divieto di trasmettere dati personali all'estero, salvo il caso in cui il destinatario si trovi in uno Stato la cui legislazione offra garanzie analoghe a quelle previste dalla presente legge.

Articolo 42.
Reciprocità tra Stati.

1) Il Ministro di Grazia e Giustizia, sentita la Commissione nazionale per la protezione dei dati personali, di cui all'art. 20, determina con proprio decreto gli Stati con i quali è ammessa la trasmissione di dati personali, previa valutazione dell'equipollenza delle singole leggi straniere.

Titolo Ottavo
Deroghe

Articolo 43.
Esenzioni.

1) Le disposizioni della presente legge non si applicano:

— ai dati personali raccolti da agenzie o organismi operanti nell'ambito delle comunicazioni giornalistiche, radiofoniche, fotografiche, televisive o cinematografiche utilizzate a fini interni, nel rispetto comunque di quanto disposto all'art. 5;

— ai dati raccolti dagli organi di polizia, dalla magistratura e dal Ministero della Difesa nell'esercizio delle proprie funzioni.

Articolo 44.
Elaborazioni di persone fisiche.

1) I dati personali detenuti da una persona fisica per l'uso privato proprio o della propria famiglia sono esentati dalle disposizioni della presente legge.

2) La persona fisica deve però poter dimostrare di aver preso le misure di sicurezza di cui all'art. 5, al fine di prevenire l'accesso o la diffusione illecita dei dati personali detenuti a scopi privati.

Articolo 45.
Indirizzari.

1) È lecito comunicare a terzi elenchi di dati relativi a persone appartenenti a specifici gruppi organizzati, purché il soggetto obbligato sia certo che gli interessati non ne subiscano nocumento e purché l'elenco contenga tassativamente nulla più di nome e cognome, data di nascita, professione, indirizzo, numero telefonico.

2) Il soggetto obbligato risponde personalmente dei danni arrecati ai singoli attraverso questa comunicazione.

Articolo 46.
Dati sensibili.

1) È fatto divieto di memorizzare dati personali relativi all'appartenenza razziale, religiosa, politica o sindacale dei cittadini, salvo che questi abbiano documentato il proprio assenso alla costituzione banche di dati personali necessarie per la gestione del proprio gruppo razziale, religioso, politico o sindacale di appartenenza.

2) È fatto divieto di memorizzare dati relativi alle abitudini sessuali dei cittadini, salvo che da parte delle strutture sanitarie ed esclusivamente per finalità di terapia, di statistica o di ricerca.

Articolo 47.
Dati sanitari.

1) L'accesso del cittadino ai dati sanitari memorizzati deve aver luogo con l'intermediazione del medico responsabile della struttura sanitaria che li detiene, per rispettare la particolare situazione in cui possa trovarsi l'interessato.

Articolo 48.
Ricerche scientifiche e di mercato.

1) I dati personali memorizzati per finalità di ricerca scientifica o di mercato devono essere memorizzati e trattati in modo da non poter arrecare danno ad alcun soggetto.

2) Questi dati devono essere anonimizzati e aggregati nella massima misura compatibile con la ricerca.

3) Questi dati sono legittimamente detenuti anche se provenienti da raccolte realizzate per finalità diverse dalla ricerca scientifica. Possono quindi essere conservati anche dopo che è venuto meno il fine previsto nella banca di dati originaria.

4) Questi dati sono sottoposti a tutte le norme della presente legge, ad eccezione di quanto previsto dall'art. 7.

Articolo 49.
Dati statistici ufficiali (Istat).

1) Le banche di dati personali usate per la preparazione di statistiche ufficiali sono soggette a tutte le norme della presente legge, ad eccezione di quella che prevede l'accesso al dato da parte dell'interessato.

2) Questa eccezione viene meno se i dati personali vengono usati o comunicati per fini diversi dall'elaborazione di statistiche ufficiali, ovvero se il risultato finale permette d'individuare direttamente o indirettamente la persona fisica interessata.

Titolo Nono
Sanzioni

Articolo 50.
Sanzioni penali.

1) Chi fraudolentemente accede, comunica, modifica, cancella o preleva, per sé o per altri, dati personali protetti dalla presente legge è punito con la reclusione fino ad un anno e con una multa da 5 a 50 milioni di lire.

2) La pena è raddoppiata se il soggetto agisce per procurare un vantaggio materiale a sé o ad altri, ovvero per arrecare un danno.

Articolo 51.
Aggravanti per la violazione del segreto professionale.

1) Agli appartenenti agli organi ed uffici previsti dalla presente legge che non rispettino il segreto d'ufficio stabilito all'art. 4, si applicano le pene stabilite dall'art. 326 cod. pen., l'immediata destituzione dall'impiego, nonché la pena accessoria dell'interdizione dai pubblici uffici.

Articolo 52.
Illeciti amministrativi dei soggetti obbligati.

1) Commette un illecito amministrativo il soggetto obbligato che:

— non informa l'interessato dell'inclusione dei suoi dati personali in una banca di dati;

— non nomina del tutto o nomina in ritardo il responsabile dei dati nell'ente pubblico o nell'impresa privata, ovvero nomina una persona i cui requisiti non corrispondono a quelli prescritti dall'art. 14, comma 3;

— non effettua del tutto o effettua in ritardo la notifica presso il garante competente, o la effettua in modo lacunoso rispetto ai contenuti prescritti dall'art. 13;

— non fornisce le informazioni richieste dai garanti, ovvero le fornisce tardive, incomplete o inesatte, ovvero ostacola l'ispezione dei locali e dei documenti d'ufficio.

2) Gli illeciti di cui al presente articolo comportano il pagamento di un'ammenda dai 2 ai 10 milioni per ogni singola infrazione.

Articolo 53.
Illeciti amministrativi degli uffici.

1) Per gli addetti agli organi e agli uffici previsti dalla presente legge che non rispettino i termini prescritti dalla medesima è prevista per ogni evento un'ammenda pari al quinto dello stipendio mensile.

Articolo 54.
Adeguamento valutario delle sanzioni.

1) Le sanzioni pecuniarie e i diritti di segreteria previsti dalla presente legge

all'inizio di ogni anno vengono ricalcolate in base all'indice Istat sull'andamento del costo della vita nell'anno precedente.

TITOLO DECIMO
Finanziamento della legge.

Articolo 55.
Copertura finanziaria.

1) La presentazione della notifica di una banca di dati personali o il suo rinnovo, di cui all'art. 12, comporta il pagamento di L. 60.000 di diritti di segreteria, indipendentemente dalle dimensioni della banca di dati e dalla durata dell'iscrizione richiesta.

2) Eventuali variazioni dei diritti di segreteria vengono proposte dalla Commissione nazionale per la protezione dei dati al Ministero di Grazia e Giustizia.

3) Le entrate derivanti dalle sanzioni amministrative previste dall'art. 52 hanno destinazione vincolata al finanziamento della presente legge.

Disposizioni transitorie e di coordinamento

Le singole attività da compiere per ottemperare alla presente legge vanno dilazionate nell'arco di almeno un anno. In questa fase è prematuro prevedere una tempificazione delle attività, dal momento che i termini prescritti nelle singole norme precedenti vanno ancora discussi.

Vanno fissati anzitutto i termini entro cui nominare il responsabile interno dell'ente o impresa; i termini entro cui adeguarsi alle misure per la sicurezza previste dall'art. 5.

Va previsto il coordinamento con la legge di riforma di pubblica sicurezza e con lo Statuto dei lavoratori.