ETTORE GIANNANTONIO

IL NUOVO DISEGNO DI LEGGE SULLE BANCHE DI DATI PERSONALI

SOMMARIO 1. Il nuovo disegno di legge sulle banche di dati personali. — 2. L'oggetto del nuovo disegno di legge. — 3. Il principio della libertà informatica. — 4. I limiti della libertà informatica. — 5. Il Garante della libertà informatica. — 6. Il diritto di accesso. — 7. La comunicazione e la diffusione dei dati. — 8. La trasmissione dei dati personali oltre frontiera. — 9. Le sanzioni penali.

1. Il nuovo disegno di legge italiano.

Con decreto del Ministro di Grazia e Giustizia in data 5 luglio 1980 veniva affidato ad una Commissione, presieduta dall'allora Primo Presidente della Corte Suprema di Cassazione Giuseppe Mirabelli, il compito di predisporre « uno schema di disegno di legge concernente la protezione delle persone di fronte ai pericoli che ad esse possono derivare dalla raccolta e gestione dei dati personali a mezzo di sistemi automatizzati anche in relazione al flusso transfrontiera degli stessi ». Lo schema, che doveva tener conto « dei principi che figurano in progetti di convenzioni ed in altri strumenti elaborati dal Consiglio d'Europa, dalle Comunità Europee e da altri enti internazionali », veniva consegnato il 20 luglio 1982 al termine dei lavori della commissione al Ministro di Grazia e Giustizia che lo presentava, con alcune modifiche di poco conto, al Parlamento il 5 maggio 1984[1].

Nel corso della IX legislatura, inoltre, venivano proposti al Parlamento alcuni disegni di iniziativa parlamentare concernenti la materia. Precisamente, il 21 aprile 1981 veniva presentata in Parlamento, ad opera del deputato Accame, la proposta di legge n. 2553 intitolata « Norme per la salvaguardia del diritto al rispetto della vita privata nei confronti dei sistemi di trattamento ed elaborazione automatica

[1] Disegno di legge n. 1657 detto disegno di legge Martinazzoli, dal nome del Ministro di Grazia e Giustizia, Mino Martinazzoli.

dei dati e delle informazioni »; il 24 febbraio 1982 veniva presentata la proposta di legge n. 3195 del deputato Picanò e altri 7 firmatari intitolata « Tutela del diritto alla riservatezza delle persone fisiche nel trattamento automatizzato dei dati e delle informazioni »; il 27 gennaio 1984 veniva presentata la proposta di legge n. 1210 del deputato Seppia e di altri 4 intitolata « Disciplina dell'uso dei sistemi informativi personali »; il 18 gennaio 1984, infine, lo stesso Picanò e altri 6 deputati presentavano la proposta di legge n. 1144 intitolata « Norme per la tutela del diritto alla riservatezza delle persone fisiche nel trattamento automatizzato dei dati e delle informazioni personali ».

Tuttavia, né il disegno di legge Martinazzoli, né le altre proposte di iniziativa parlamentare sono state approvate dal Parlamento; e lo scadere della nona legislatura ha comportato la decadenza di tutte queste iniziative legislative[2].

Nel corso della X legislatura è stata presentata alla Presidenza della Camera una proposta di legge di iniziativa parlamentare volta a regolamentare l'uso dei sistemi informativi personali (A.C. 552); tuttavia la proposta di legge, assegnata alla seconda commissione Giustizia, alla data del 7 maggio 1990 non era stata ancora esaminata.

Con decreto in data 4 febbraio 1988 il Ministro di Grazia e Giustizia istituiva un gruppo di studio con l'incarico di procedere alla revisione e all'aggiornamento del disegno di legge n. 1657[3].

Il gruppo di studio, dopo avere ascoltato i rappresentanti delle associazioni delle categorie maggiormente interessate alla materia, ha prospettato al Ministro l'esigenza che la disciplina della materia, sia pure nel rispetto dei principi enunciati nella Convenzione di Strasburgo, fosse ispirata a criteri sostanzialmente diversi da quelli in base ai quali era stato redatto il d.d.l. n. 1657; e ciò per la rilevante evoluzione avvenuta dopo l'elaborazione del detto disegno di legge in relazione sia al progresso dei mezzi tecnici che alle esigenze sociali.

Il gruppo di lavoro ha quindi proceduto, dietro ulteriore invito del Ministro, alla redazione di un nuovo disegno di legge ispirato ai seguenti principi fondamentali: *a*) esonero dall'obbligo di notificazione per le raccolte destinate a scopi privati e professionali; *b*) obbligo di notificazione e normativa di controllo soltanto per le banche di dati

[2] In effetti nella seduta del 1° ottobre 1986 la IV Commissione Permanente della Camera dei Deputati, Giustizia, aveva iniziato, in sede referente, l'esame del Disegno di legge n. 1657 e delle proposte Picanò e Seppia. Il relatore, on. Violante, dopo avere sottolineato il ritardo con il quale in Italia veniva affrontata la disciplina della materia, auspicava che il previsto organo di controllo fosse designato dal Parlamento e che venisse istituito un procedimento snello di registrazione ed un equilibrato sistema sanzionatorio; proponeva, poi, che venisse istituito un Comitato ristretto che procedesse ad audizioni di esperti della materia. Su tale proposta concordava il Presidente della Commissione, che sottolineava anche l'opportunità di visite di studio in Paesi stranieri.

L'esame dei progetti di legge era quindi rinviato ad altra seduta, ma la legislatura si chiudeva senza che la materia fosse stata ripresa in esame.

[3] Il Gruppo di studio, costituito da un ristretto numero di giuristi, era presieduto dallo stesso Primo Presidente emerito della Corte Suprema di Cassazione, Prof. Giuseppe Mirabelli.

destinate alla comunicazione a terzi; *c*) normativa particolare per i c.d. dati sensibili; *d*) disciplina rigorosa per le banche pubbliche di dati; *e*) indipendenza dell'organo di controllo dal Governo; *f*) esclusione dell'obbligo di comunicazione preventiva all'interessato.

Il 30 settembre 1989 il gruppo di studio ultimava i suoi lavori e rimetteva al Ministro Giuliano Vassalli il testo definitivo della relazione e dello schema del disegno di legge concernente la disciplina delle banche di dati personali ad elaborazione informatica.

Nelle more dei lavori del gruppo il Parlamento approvava la legge 21 febbraio 1989, n. 98 con la quale il Presidente della Repubblica veniva autorizzato a ratificare la Convenzione di Strasburgo[4].

L'approvazione della legge, peraltro, non ha sanato l'inadempienza dell'Italia nei confronti della Convenzione ed, anzi, è stata oggetto di ulteriori commenti sfavorevoli nell'ambito internazionale.

In base agli artt. 4 e 22 della Costituzione, infatti, la ratifica presuppone l'emanazione di una normativa interna conforme ai principi contenuti nella Convenzione stessa, non potrebbe essere effettuata finché non venga emanata tale normativa e, se effettuata, è del tutto inutile[5].

[4] In effetti, già nella IX legislatura e, precisamente, il 26 maggio 1986, era stato presentato alla Camera, ad iniziativa del Ministero degli Affari Esteri, il disegno di legge n. 3793, concernente la ratifica e l'esecuzione della Convenzione di Strasburgo, nella cui relazione veniva peraltro precisato che la ratifica era subordinata all'introduzione nell'ordinamento italiano di una disciplina organica della materia e veniva segnalato il collegamento con il disegno di legge n. 1657.

La chiusura della legislatura aveva comportato la decadenza del disegno di legge e pertanto nella X legislatura, il 15 dicembre 1987, era stato presentato alla Camera dei Deputati, ad iniziativa del Ministero degli Affari Esteri, di concerto con il Ministro dell'Interno e con il Ministro di Grazia e Giustizia, un disegno di legge che riproduceva nella relazione e nel testo il precedente disegno di legge n. 3793 e che sarebbe divenuto, appunto, la legge 21 febbraio 1989, n. 98 intitolata « Ratifica ed esecuzione della Convenzione di Strasburgo del 28 gennaio 1981 ».

[5] L'art. 4 della Convenzione dispone: — « Impegni delle Parti. — 1) Ciascuna Parte adotta, nell'ambito del suo diritto interno, le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati enunciati nel presente capitolo.

2) Tali misure devono essere adottate al più tardi al momento dell'entrata in vigore della presente convenzione rispetto a tale Parte ».

La norma deve essere posta in collegamento con l'art. 22 che stabilisce il momento dell'entrata in vigore della Convenzione rispetto a ciascuno Stato: — Art. 22 — « Entrata in vigore.

1) La presente Convenzione è aperta alla firma degli Stti membri del Consiglio d'Europa. Essa sarà sottoposta a ratifica, accettazione o approvazione. Gli strumenti di ratifica, d'accettazione o di approvazione saranno depositati presso il Segretario Generale del Consiglio d'Europa.

2) La presente convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data in cui cinque Stati membri del Consiglio d'Europa avranno espresso il loro consenso ad essere vincolati dalla convenzione in conformità alle disposizioni del comma precedente.

3) Per ogni Stato membro che esprimerà successivamente il suo consenso ad essere vincolato dalla Convenzione, questa entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data del deposito dello strumento di ratifica, di accettazione o di approvazione.

L'Italia ha, invece, operato nel senso opposto: la ratifica ha preceduto la regolamentazione interna e, pertanto, rimane inoperante finché non venga emanata tale regolamentazione.

È evidente quindi che la legge di ratifica non ha eliminato la necessità di una disciplina delle banche di dati in Italia, ma, anzi, l'ha resa più urgente; e tale carattere di urgenza è stato sottolineato dalle stesse associazioni imprenditoriali. Queste, nelle audizioni compiute da parte della Commissione, hanno osservato che la mancanza di esecuzione della Convenzione porrà le imprese italiane nella impossibilità di avvalersi dell'accordo internazionale nell'attività di trasmissione e di ricezione dei dati attraverso le frontiere; e che tale impossibilità risulterà particolarmente sfavorevole alla data dell'entrata in vigore dell'atto unico di integrazione europea, previsto per la fine del 1992.

Al riguardo, va osservato, peraltro, che la raccomandazione della Commissione della Comunità Europea prevedeva che « se entro un lasso di tempo ragionevole la firma e la ratifica della convenzione da parte degli Stati membri non avrà luogo, la Commissione si riserva di proporre al Consiglio l'adozione di un atto giuridico basato sul trattato Cee ».

In base a tale previsione il 24 settembre 1990 è stata formulata una proposta di direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali. La direttiva ha per oggetto la predisposizione di una protezione di equivalente livello in tutti gli Stati membri della Comunità al fine di eliminare gli ostacoli agli scambi di dati necessari al funzionamento del mercato interno[6].

[6] La proposta è destinata ad essere integrata da una serie di misure complementari e precisamente:

a) un progetto di risoluzione dei rappresentanti degli Stati membri delle Comunità Europee per estendere l'applicazione dei principi della direttiva generale agli archivi del settore pubblico non contemplati dalla direttiva, ossia agli archivi delle amministrazioni le cui attività non rientrano nel campo del diritto comunitario;

b) una dichiarazione della Commissione che auspica che i principi della direttiva si applichino alle istituzioni e agli organismi della Comunità;

c) una proposta di direttiva del Consiglio sulla protezione dei dati a carattere personale e sulla tutela della riservatezza nell'ambito delle reti digitali pubbliche di telecomunicazioni, con particolare riferimento all'ISDN (rete digitale integrata nei servizi) e alle reti digitali per servizi di radiotelefonia mobile. La direttiva mira a garantire agli utilizzatori in tutti gli stati membri un livello di base di protezione mediante misure che debbono essere integrate nei servizi offerti dalle nuove reti;

d) una raccomandazione di decisione del Consiglio concernente l'adesione della Comunità Europea alla Convenzione del Consiglio d'Europa. L'adesione alla Convenzione garantirà nelle relazioni tra la Comunità ed i paesi terzi aderenti la protezione delle persone interessate e la circolazione oltre frontiera dei dati personali;

e) una proposta di decisione del Consiglio concernente l'adozione di un piano di azione di due anni in materia di sicurezza dei sistemi di informazione.

2. L'OGGETTO DEL NUOVO DISEGNO DI LEGGE.

L'art. 1 definisce alcune nozioni fondamentali per la interpretazione della legge come quelle di elaborazione informatica, di dato personale, di titolare della banca, di interessato, di comunicazione e di diffusione.

La tecnica di definire preliminarmente gli istituti disciplinati è moderna ed è particolarmente giustificata nel caso in cui la legge intervenga su materie nuove, non regolate per il passato e in cui non vi è una terminologia universalmente accettata.

Particolare importanza hanno le prime tre definizioni di « banca di dati » (« qualsiasi raccolta sistematica di informazioni »), di « elaborazione informatica » (« ogni operazione svolta in tutto o in parte con mezzi elettronici o, comunque, automatizzati, concernenti la registrazione, la modificazione, il trattamento logico, la comunicazione e la diffusione dei dati ») e di « dato personale » (« ogni informazione relativa a persona fisica, persona giuridica o ente di fatto che sia idonea, comunque, a consentirne l'identificazione »).

Le tre nozioni, benché distinte, delimitano l'oggetto della legge che riguarda sempre ed esclusivamente le banche di dati personali ad elaborazione informatica. Sono pertanto escluse dalla disciplina sia le raccolte non automatizzate di dati personali sia le raccolte di dati non personali.

È stato, tuttavia, osservato che l'espressione « banca di dati » è in contrasto con l'art. 2 della legge bancaria n. 375 del 1936 che proibisce l'uso del termine « banca » in senso diverso da quello di istituto di credito[7]; che tale espressione costituisce la traduzione dell'inglese « data bank » e che nel disegno di legge è usata in senso improprio per indicare qualsiasi raccolta sistematica di informazioni.

In particolare è stato osservato che occorre distinguere l'archivio, manuale, elettronico o circuitale che dir si voglia, dalla base di dati (data base) e dalla banca di dati; che una raccolta sistematica di informazioni, così come intesa dal disegno di legge, costituisce un archivio, ma non necessariamente una base di dati o una banca di dati; che con quest'ultime espressioni si deve intendere, invece, « un insieme di informazioni non duplicate, in correlazione reciproca ed utilizzabili per più applicazioni e da più utenti »; e che, ai fini del disegno di legge, l'espressione banca di dati dovrebbe essere limitata a quelle sole grandi banche di dati personali in cui appositi programmi di elaborazione informatica assicurino un valore ag-

[7] ... Le parole Banca, Banco, Cassa di Risparmio, Credito, Risparmio e simili non potranno in alcun caso usarsi nella denominazione di isituti, enti o imprese che non siano soggette al controllo dell'ispettorato o che comunque non ne abbiano avuto l'autorizzazione... (art. 2 legge 375/1936).

giunto all'informazione e una possibilità di conoscenza altrimenti impossibili[8].

È stato d'altra parte contrapposto che l'espressione « data bank » in termini generali è entrata nell'uso comune e nelle varie normative, anche comunitarie, che sono intervenute in materia.

Non tutte le normative, peraltro, identificano il loro oggetto negli stessi termini del disegno di legge italiano: alcune, infatti, estendono la nozione di banca di dati anche agli archivi non automatizzati; ed altre la restringono ai soli dati relativi alle persone fisiche, con esclusione quindi dei dati relativi alle persone giuridiche, alle imprese e ad altre figure soggettive.

L'estensione della tutela a soggetti diversi dalla persona fisica è prevista, ad esempio, nella legge norvegese[9], danese[10], austriaca[11] e

[8] BORRUSO, *Computer e diritto*, vol. II, p. 384, Giuffrè, Milano, 1988. Lo stesso autore afferma che « una banca di dati può essere definita tale solo quando consente almeno la realizzazione dei seguenti cinque principi fondamentali che rivoluzionano totalmente la tecnica della ricerca e consentono di ottenere risultati efficacissimi dal punto di vista della ricchezza di informazioni: ...1) libertà e causalità della ricerca... 2) libera combinazione delle chiavi di ricerca in and, or, not secondo le regole della logica booleana; 3) libere mascherabilità di caratteri alfanumerici di un dato chiave... 4) possibilità di estrarre automaticamente informazioni dai documenti registrati e di ottenerne la prospettazione in forma sintetica; 5) possibilità di interagire con il *computer* svolgendo la ricerca con una serie successiva di ordini e di dati... (BORRUSO, TIBERI, *L'informatica per il giurista*, p. 190, Giuffrè, Milano, 1990).

[9] Art. 1 legge norvegese 9 giugno 1978 n. 48 sui registri di dati personali:

La legge si applica ai registri di dati personali ed altre utilizzazioni di informazioni personali in certi tipi di attività. Per informazioni personali si intendono informazioni e valutazioni le quali direttamente o indirettamente possono essere collegate a singole persone identificabili, associazioni o fondazioni.

Per registri di dati personali si intendono registri, archivi, elenchi eccetera in cui sono raccolte sistematicamente informazioni personali in modo che le informazioni sulla singola persona possano essere ritrovate. La legge si applica ai registri di dati personali delle amministrazioni statali o comunali, delle imprese private, associazioni e fondazioni...

[10] Art. 1 legge danese 8 giugno 1978, n. 293 sui registri privati:

« 1) Le registrazioni di dati personali effettuate a mezzo di elaboratori elettronici, nonché le registrazioni sistematiche di dati personali o finanziari relativi a ogni individuo, istituzione, associazione o impresa commerciale e altri dati relativi a caratteristiche personali di cui si può ragionevolmente esigere che non siano rese di pubblico dominio possono essere effettuate unicamente in conformità ai capitoli due e tre della presente legge.

2) Ai fini dell'applicazione della presente legge, si intendono per dati di carattere personale i dati riferibili ad una persona identificabile, anche se il riferimento suppone la conoscenza del numero di codice personale o di ogni altro mezzo di identificazione della persona in questione.

[11] Art. 3 legge austriaca 18 ottobre 1978, n. 656 sulla protezione di dati personali (Datenschutzgesetz):

Ai sensi della presente legge si intendono per:

1) Dati — dati immagazzinati in un raccoglitore che rappresentano informazioni su una persona fisica o giuridica o una società commerciale determinata o determinabile (dati individuali);

2) Interessati — persone fisiche, giuridiche o società commerciali in riferimento alle quali i dati vengono raccolti, elaborati o trasmessi...

lussemburghese[12]; non è prevista, invece, nella legge svedese[13], tedesca[14], francese[15] e in quella del Regno Unito[16].

Particolarmente interessanti sono, sotto questo aspetto, le leggi israeliana e francese. La prima perché esclude espressamente che il termine « persona » comprenda le persone giuridiche[17]; la seconda perché precisa che l'oggetto della legge riguarda i dati relativi a persone fisiche « sia che l'elaborazione sia effettuata da una persona fisica sia da una persona morale ».

La legge del Regno Unito comprende, inoltre, tra i dati personali « qualsiasi espressione di opinione riguardante la persona stessa, ma senza indicazione delle "intentions" dell'utente dei dati nei confronti di quest'ultima ». In tal modo, è stato osservato, sono compresi nell'oggetto della legge i giudizi altrui riguardanti un individuo, ma non i giudizi espressi dall'utente dei dati nei confronti dell'individuo stesso. Perciò la frase « si ritiene che il signor Bloggs non meriti fiducia » sarà compresa, ma non la frase « non intendiamo dar fiducia al signor Bloggs »[18].

[12] Art. 2 della legge lussemburghese 31 marzo 1979 sull'utilizzazione dei dati normativi nei sistemi informatici:

« Ai fini dell'applicazione della presente legge i termini appresso elencati hanno il seguente significato:

Dato nominativo: ogni informazione riguardante una persona che è o può essere determinata;

Persona: ogni persona fisica o giuridica, pubblica o privata o società di fatto;

Banca di dati: raccolta di dati di base registrati su un supporto informatico...

[13] Art. 1 della legge svedese 11 maggio 1973, n. 289 (Datalag):

« Ai fini della presente legge si intende per:

dati personali (personuppgift) le informazioni concernenti un individuo (persona fisica);

archivio di dati personali (personregister) ogni archivio, lista o altra registrazione tenuta mediante un sistema di elaborazione automatica dei dati e contenente dati personali riferibili alla persona interessata...

[14] Art. 2 legge tedesca 27 gennaio 1977 sulla protezione dei dati personali:

« Definizioni concettuali

1) Ai fini delle presente legge devono considerarsi dati ed informazioni personali tutti quei dati che si riferiscono ai rapporti, di natura personale o reale, che abbiano quale centro di imputazione una persona fisica determinata o determinabile (interessata)...

[15] Art. 4 della legge francese 6 gennaio 1978, n. 78-17:

« Sono ritenute nominative ai sensi della presente legge le informazioni che permettono sotto qualsiasi forma, direttamente o no, la identificazione della persone fisiche alle quali esse si applicano, sia che l'elaborazione sia effettuata da una persona fisica sia da una persona morale ».

[16] Art. 1 del Data Protection Act del Regno Unito:

« 1) Ai fini della presente legge valgono le seguenti disposizioni:

2) Dati (data): indica le informazioni registrate in forma tale che esse possano venire elaborate mediante l'impiego di apposite apparecchiature che funzionano automaticamente in risposta ad istruzioni all'uopo fornite.

3) Dati personal (Personal data): indica dati costituiti da informazioni relative a persona vivente che possa essere identificata attraverso di esse, ivi compresa qualsiasi espressione di opzione riguardante la persona stessa, ma senza indicazione delle « intentions » dell'utente dei dati nei confronti di quest'ultima...

[17] Art. 3 della legge israeliana sulla protezione della vita privata:

« Definizioni dei termini. — Ai fini della presente legge:

il termine persona, ai sensi degli artt. 2, 7, 13, 14 e 25 non comprende le persone giuridiche...

[18] CHALTON, *Il Data Protection Act inglese*, in questa *Rivista*, 1986, p. 103.

Infine alcune leggi come quella israeliana contengono un elenco dei dati personali[19].

Per quanto riguarda l'elaborazione dei dati la maggioranza delle legislazioni limita la disciplina alle raccolte automatizzate di dati personali. Alcune, tuttavia, come la legge tedesca e quella austriaca, l'estendono anche alle raccolte manuali. Dispone, ad esempio, l'art. 2 della legge tedesca del 27 gennaio 1977: « una banca di dati è una raccolta di dati fatta con criteri di uniformità e che può essere ordinata e impostata secondo caratteristiche determinate e riordinata e utilizzata secondo altre caratteristiche indipendentemente dal procedimento adottato al riguardo; non rientrano in quest'ambito gli atti e le raccolte di atti, a meno che non possano essere riordinati ed utilizzati con procedimenti automatizzati ».

3. Il principio della libertà informatica.

I punti principali in cui si articola il disegno di legge sono: la disciplina della raccolta dei dati personali e della formazione della banca dei dati (artt. 2-8), la istituzione del Garante per l'attuazione della legge (artt. 9-11), la disciplina della comunicazione e della diffusione dei dati (artt. 14-19), la trasmissione dei dati personali oltre frontiera (art. 20), le sanzioni penali (artt. 21-23), le disposizioni transitorie e particolari (artt. 24-27).

Per quanto riguarda la disciplina della formazione delle banche di dati personali si possono distinguere due generazioni di leggi.

La prima è costituita da quelle normative, particolarmente severe, che vietano qualsiasi raccolta automatizzata di dati personali non espressamente e specificamente autorizzata con una legge o con un provvedimento amministrativo.

Alla base di queste normative vi è, in sostanza, un profondo timore del legislatore nei confronti dell'elaboratore: uno strumento, ancora in gran parte sconosciuto, che può dar luogo a danni ingenti e imprevedibili.

Appartengono a questa generazione la prima legge svedese, la « Datalag » emanata l'11 maggio 1973, la « Bundesdaten Schutzge-

[19] Art. 7 della legge israeliana:
« il termine informazioni sta ad indicare dati sulla personalità, lo *status* personale, gli affari intimi, lo stato di salute, la posizione economica, le qualifiche professionali, le opinioni ed i convincimenti di una persona...

setz » (BDSG) tedesca, la « Datenschutzgesetz » (DSG) austriaca[20].

Criteri restrittivi in materia di costituzione di banche di dati personali sono anche contenuti nelle legislazioni danese (art. 4 e art. 6), norvegese (art. 6) e islandese.

La seconda generazione di leggi in materia di raccolte di dati personali è costituita, invece, da quelle norme, più liberali, per le quali ciascuno può costituire raccolte automatizzate di dati, anche personali, senza necessità di alcuna autorizzazione, salvo l'obbligo di darne notificazione ad un particolare organo o ufficio, come il Datainspektionen della seconda legge svedese, il Data Protection Registrar britannico o il Registrar israeliano.

Principio fondamentale di tali norme, infatti, non è quello di vietare tutte le raccolte di dati non espressamente e specificamente autorizzate, ma, al contrario, di riconoscere la libertà di raccolta dei dati personali e sottoporre tale libertà ad una serie di limiti e di oneri, primo tra tutti quello della notificazione della banca all'Ufficio di controllo.

Il compito di quest'ultimo Ufficio è quello non di autorizzare, ma di controllare che le informazioni siano state ottenute in modo legittimo[21].

[20] Ad esempio l'art. 6 della DSG austriaca dispone che « ai fini della circolazione di dati elaborati utilizzando procedimenti automatizzati, i dati possono essere raccolti o elaborati solo in presenza di una autorizzazione legislativa esplicita o se ciò costituisce per il committente presupposto essenziale per l'attuazione dei compiti ad esso demandati dalla legge (art. 6 Datenschutzgesetz).

Parimenti restrittiva e la normativa tedesca in cui « L'elaborazione dei dati personali è consentita solamente se: 1) la presente legge od un'altra disposizione normativa lo consente; 2) l'interessato ha prestato il suo consenso.

Il consenso deve essere prestato per iscritto a meno che, a causa di speciali circostanze, non sia opportuna una forma diversa; se il consenso viene rilasciato congiuntamente ad altre dichiarazioni, l'interessato deve essere specificamente informato al riguardo per iscritto (art. 3) ».

Anche per la legislazione lussemburghese « l'istituzione e la gestione di ogni banca di dati non dipendente dallo Stato sono sottoposte all'autorizzazione preliminare del ministro nelle attribuzioni del quale rientra la tenuta del registro nazionale delle banche di dati previsto dall'art. 13 » (art. 4 legge 31 marzo 1979).

[21] Dispone, ad esempio, la legge israeliana che « l'organo al quale è stata notificata la costituzione di una banca di dati *deve* procedere alla registrazione, a meno che esso non ravvisi una causa ragionevole per ritenere che la banca serva di copertura per attività illecite » (art. 10 della legge israeliana). E, ai fini del controllo, l'allegato 1 della legge britannica precisa che « nello stabilire se le informazioni siano state ottenute in modo legittimo si dovrà tenere conto dei seguenti elementi:

a) il fine o i fini per i quali si intende raccogliere le informazioni;

b) i mezzi con cui esse sono state ottenute, accertando in particolare se la persona da cui sono state ottenute sia stata tratta in inganno o fuorviata quanto allo scopo o agli scopi perseguiti ».

Particolarmente interessante a questo riguardo è la seconda legge svedese. Tutti coloro, soggetti pubblici o privati, che intendono formare o gestire archivi di dati personali devono chiedere la licenza (licens) o l'autorizzazione (tillstand) quando l'archivio che si vuole formare riguarda dati particolarmente sensibili.

La licenza o l'autorizzazione sono rilasciate da un apposito organo, l'Ispettorato dei dati (Datainspektionen): la licenza è un atto dovuto, l'autorizzazione è concessa solo quando non sussistono motivi di temere una violazione della privacy e può essere subordinata al rispetto di eventuali direttive.

In ogni caso (art. 7) gli archivi di dati personali devono essere formati e tenuti in modo che non si verifichi un'indebita invasione nella riservatezza della persona registrata. A questo riguardo speciale attenzione deve esse-

Tra le normative più liberali della seconda generazione rientrava anche il disegno di legge Martinazzoli per il quale chiunque poteva costituire banche di dati salvo l'obbligo di notificazione all'Ufficio di controllo. In particolare la relazione della Commissione al disegno di legge affermava più volte che la scelta fondamentale del disegno era « quella della libertà della raccolta dei dati e della loro circolazione »; che « al fine di assicurare un efficace sistema di controlli, senza limitare l'esercizio della libertà informatica, né introdurre procedure eccessivamente macchinose, la Commissione ha scartato l'ipotesi di sottoporre a regime autorizzativo le banche dei dati, recependo, invece, il sistema della notificazione già introdotto dalla legge 1° aprile 1981, n. 121 »; che « se la scelta fondamentale è quella della libertà della raccolta dei dati e della loro circolazione, questi debbono tuttavia essere qualificati, nel senso della pertinenza allo scopo, della loro esattezza ed attualità, del loro impiego funzionale allo scopo, con durata limitata nel tempo ».

Tuttavia, nonostante i suoi meriti, il disegno di legge Martinazzoli è stato sottoposto, sin dal primo momento, a numerose critiche[22] soprattutto per il suo carattere di normativa generale. Esso, infatti, sottoponeva, al pari delle altre leggi europee di quel periodo, ad una stessa disciplina qualsiasi tipo di banca di dati. Ed è stato osservato che una disciplina uniforme può risultare, a seconda dei casi, talvolta appena sufficiente, tal'altra eccessiva e tal'altra ancora addirittura assurda; che il numero delle banche di dati avrebbe reso inapplicabile la legge e avrebbe paralizzato l'attività dell'ufficio di controllo; che le sanzioni previste erano particolarmente gravi e potevano colpire, anche in mancanza di dolo o colpa, tutti coloro che avessero pensato di utilizzare un elaboratore sia pure per divertimento ovvero per lo svolgimento della propria attività professionale.

In realtà il disegno di legge Martinazzoli presupponeva una realtà informatica molto diversa da quella attuale, una realtà caratterizzata dalla presenza di poche banche di dati di grandi dimensioni per la cui gestione occorreva una notevole capacità tecnica e una grande possibilità economica.

La normativa che si pensava di introdurre prevedeva, quindi, da un lato un penetrante e capillare potere di controllo da parte di un organo pubblico appositamente costituito; dall'altro il riconoscimento di una serie di vasti e rilevanti diritti dell'individuo interessato come il diritto di accesso e il diritto alla comunicazione.

re rivolta ai seguenti punti:

1) l'archivio deve essere tenuto per uno scopo specifico;

2) nessun dato può essere registrato se non conforme allo scopo dell'archivio;

3) i dati personali non possono essere raccolti, diffusi o altrimenti utilizzati se non in conformità allo scopo dell'archivio o in base a disposizioni di legge o altre disposizioni o con il consenso della persona registrata;

4) i dati contenuti nell'archivio devono essere protetti contro la distruzione illecita o involontaria o contro l'alterazione o la diffusione illecita.

[22] Una raccolta sistematica di tali critiche è contenuta in *Mirabelli G., Osservazioni e rilievi allo schema di DDL sulle banche di dati*, in *Quaderni della giustizia*, n. 31 p. 25.

La nuova realtà informatica, quale si è venuta a creare alla fine degli anni '70, a seguito soprattutto dell'introduzione dei c.d. « personal computers » è, invece, notevolmente diversa ed è caratterizzata, ormai, da una miriade incalcolabile e incontrollabile di piccole banche di dati che utilizzano apparecchi di dimensioni e di costi modesti. « Il computer » da strumento di pochi è divenuto il modo di lavorare di tutti o, come è stato incisivamente detto, la penna e il quaderno dei giorni nostri. Ciò ha reso da una parte impossibile il controllo di ciascuna banca di dati personali ad opera di un organo pubblico a ciò preposto, qualunque sia la dotazione di mezzi o di personale per esso prevista; dall'altra ha trasformato il diritto di accesso, di comunicazione e le altre situazioni giuridiche attive, riconosciute a ciascun individuo come mezzo di tutela della propria libertà nei confronti dei detentori del potere informatico, in potenziali strumenti di violazione di quella libertà di pensiero e di riservatezza che tutti devono avere nello svolgimento della propria attività, professionale o imprenditoriale, anche se usano mezzi informatici.

Inoltre, come è stato affermato nella relazione del gruppo di lavoro, « il crescente bisogno di informazione, sempre più presente in ogni individuo, per l'esigenza di indirizzare adeguatamente le proprie attività personali e professionali ed il bisogno, parimenti crescente, della collettività organizzata di acquisire una gamma sempre più vasta di informazioni, al fine di effettuare meditate scelte politiche e di produrre adeguati sistemi di organizzazione, hanno progressivamente determinato la prevalenza dell'interesse all'informazione sull'interesse alla c.d. riservatezza... ». L'interesse ad essere informato si è palesato inerente alla stessa personalità di ogni individuo, sicché una indiscriminata compressione di questo interesse è apparsa come lesiva del diritto fondamentale di libertà.

È sembrato necessario, quindi, acquisire una nozione di libertà informatica in senso opposto a quello che era stato in precedenza prospettato da taluno: non « libertà di non essere assoggettati al potere informatico altrui », ma « libertà di adoperare senza vincoli ingiustificati i mezzi informatici per le proprie personali esigenze ».

È questa, infatti, la regola fondamentale che il gruppo ha ritenuto dovesse essere enunciata e che è contenuta nell'art. 2 del nuovo disegno di legge: « chiunque ha il diritto di raccogliere dati, assoggettarli ad elaborazione informatica e utilizzare i dati raccolti ed elaborati allo scopo di soddisfare interessi personali, nell'ambito della propria vita privata e della propria attività professionale e imprenditoriale »[23].

[23] Anche il vecchio disegno di legge affermava il principio della libertà informatica, ma questo solo per dire che la creazione di una banca di dati non richiedeva necessariamente una preventiva autorizzazione; peraltro il disegno di legge finiva per addossare a chiunque una pluralità di obblighi, da quello di notifica o di accesso a quello, particolarmente gravoso, della comunicazione.

Nel nuovo disegno di legge, invece, l'affermazione del principio di libertà informatica assume un valore del tutto diverso e sta a significare che la costituzione di una banca di dati è perfettamente libera qualora sia destinata all'uso personale e rientri nell'ambito della propria vita privata o della propria attività professionale e imprenditoriale.

La disciplina della notificazione e dell'accesso viene quindi limitata alle banche di dati personali ad elaborazioni informatica destinate alla comunicazione o alla diffusione dei dati e alle banche che contengono particolari specie di dati personali come, ad esempio, i dati sensibili o i dati sanitari.

Conseguenze del principio della libertà di raccolta dei dati per uso personale sono:

a) che i dati personali raccolti devono essere pertinenti all'uso personale e non eccedenti in relazione a tale uso (arg. *ex* art. 7);

b) che il titolare della banca di dati non può comunicare o diffondere i dati ed « è tenuto ad adottare tutte le misure occorrenti perché venga impedito che altri soggetti vengano comunque a conoscenza dei dati contenuti nella banca » (art. 2, comma 3).

Nel caso che il titolare della banca preveda di dover comunicare o diffondere i dati raccolti egli dovrà procedere all'adempimento delle formalità previste dalla legge ed in primo luogo alla notificazione al Garante (art. 4).

Peraltro sia l'attività professionale sia quella imprenditoriale possono essere svolte in organizzazioni professionali o in organismi societari o in altre organizzazioni di gruppo. A tal fine il comma 2 dell'art. 2 precisa la nozione di utilizzazione professionale e imprenditoriale sancendo che è tale anche quella compiuta in collaborazione con altri. Così ad esempio non sono banche di dati destinate alle comunicazioni a terzi quelle costituite da una associazione di istituti di credito o da un consorzio di imprese assicurative per i soli fini istituzionali degli enti membri[24].

Il concetto di uso personale della raccolta dei dati e di normale attività professionale o imprenditoriale è dunque uno dei concetti fondamentali del nuovo disegno di legge, ne costituisce uno dei tratti distintivi più evidenti rispetto al precedente e, insieme con l'altro concetto di banche di dati destinati alla comunicazione o alla diffusione, definisce il campo di applicazione della normativa.

Il concetto si trova enunciato per la prima volta nella legge danese ed è stato ripreso da due leggi recenti, quella finlandese e quella olandese[25].

Peraltro ad un esame più attento ci si può accorgere che lo stesso concetto è alla base di quelle normative che prevedono il sistema dell'autorizzazione. Questa, infatti, avrebbe dovuto essere concessa solo nel caso, appunto, che la raccolta rientrasse nel normale svolgimento dell'attività professionale o imprenditoriale di colui che richiedeva l'autorizzazione, e, nel caso di organi pubblici, se la raccolta dei dati

[24] Ministero di Grazia e Giustizia, Relazione del gruppo di studio istituito con d.m. 4 febbraio 1988 per la revisione e l'aggiornamento del disegno di legge avente ad oggetto la costituzione e l'esercizio delle banche di dati personali ad elaborazione informatica, p. 10.

[25] Legge finlandese 30 aprile 1987, n. 471 art. 1; legge dei Paesi Bassi 28 dicembre 1988, n. 665 alla sezione 2 n. 1 lettera *a*).

« è necessaria per il corretto adempimento dei compiti che rientrano nella competenza dell'ufficio »[26].

Nei riguardi del concetto di uso personale potrebbe tuttavia essere sollevata una serie di rilievi critici. Potrebbe, innanzitutto, osservarsi che si tratta di un concetto non preciso, ma vago ed elastico si da potere dar luogo a serie difficoltà nell'applicazione della legge; che di qualsiasi raccolta di dati personali si può facilmente predicare, più o meno fondatamente, che è necessaria o quantomeno utile per lo svolgimento della propria attività professionale o imprenditoriale; e che, infine, anche lo svolgimento di quest'ultima richiede quasi sempre necessariamente la comunicazione dei dati raccolti a terzi.

In effetti il concetto di uso personale potrebbe essere oggetto di una vasta gamma di interpretazioni, da quella ristretta che lo vuole limitato a quei casi nei quali « è poco probabile che sorga il rischio di violazioni di dati per fini assolutamente privati come è il caso dell'agenda elettronica personale » a quella più ampia che finirebbe per ricomprendere ogni attività professionale o imprenditoriale, anche quella delle aziende destinate alla raccolta dei dati a fini di comunicazione o di diffusione.

Senonché il lamentato carattere di indeterminatezza viene molto mitigato qualora si consideri che il concetto di uso personale deve essere inteso in relazione ai normali usi professionali o imprenditoriali; che pertanto rientrano nel principio di libertà informatica non tutte le raccolte di dati che possano essere in qualche modo utilizzate per scopi personali, ma solo quelle che rientrano nella normale attività professionale o imprenditoriale; e che comunicare i dati a terzi non fa

[26] La normativa tedesca, ad esempio, precisa i limiti in cui l'autorizzazione va concessa: « La memorizzazione e modificazione dei dati relativi a persone è consentita se è necessaria per un corretto adempimento dei compiti propri dell'unità di memorizzazione. Se i dati vengono rilevati in base ad una disposizione di legge direttamente presso una persona, questa deve essere specificamente informata della disposizione o altrimenti della volontarietà delle sue indicazioni (art. 9). La trasmissione di dati personali ad autorità o ad altri uffici pubblici è consentita se è necessaria per il corretto adempimento delle funzioni di competenza dell'ufficio che li deve trasmettere o dell'ufficio che li riceve (art. 10). La trasmissione dei dati personali ad altri uffici diversi da quelli indicati nell'art. 10 è consentita se essa è necessaria per il corretto adempimento dei compiti che rientrano nella competenza dell'ufficio che li deve trasmettere o se chi li riceve dimostra un legittimo interesse alla conoscenza dei dati da trasmettere o conseguentemente non vengono pregiudicati gli interessi, meritevoli di tutela, dell'interessato ».

Per la legge norvegese la registrazione di dati personali deve essere giustificata da ragioni obiettive, con riguardo alle attività amministrative ed operative dell'istituzione o dell'impresa che effettua le registrazione (art. 6).

Per la legge islandese la registrazione sistematica dei dati personali è consentita solo nei casi in cui la registrazione stessa costituisce parte normale delle attività del soggetto interessato e si estenda esclusivamente a coloro che sono collegati alla sfera di attività di esso e cioè i clienti, i dipendenti o i soci (art. 3).

Per la legge danese le imprese commerciali, i commercianti, le istituzioni, le associazioni e simili possono effettuare registrazioni di dati personali a mezzo di elaboratori elettronici unicamente nella misura in cui la registrazione fa parte del normale esercizio dell'impresa della categoria in questione.

venir meno il principio di libertà informatica qualora tale attività di comunicazione rientri anch'essa nell'ambito della normale attività professionale o imprenditoriale.

Potrebbe d'altra parte osservarsi che l'esclusione delle banche di dati ad uso personale dalla disciplina della legge costituisce una grave limitazione di questa e si pone in contrasto con la Convenzione Europea che sembra riferirsi ad ogni raccolta di dati personali. Senonché tale contrasto non sembra sussistere in quanto, come si è visto, sia la legge danese, sia quella finlandese e olandese, pur utilizzando lo stesso concetto di uso personale per escludere l'applicabilità della legge, non sono state perciò ritenute contrarie alla Convenzione[27].

Occorre infine osservare che il disegno di legge finisce per non comprendere una serie di banche di dati personali per le quali si presenta pur sempre necessaria una adeguata disciplina.

Difatti, tra le banche di dati personali destinate allo scopo di soddisfare interessi personali da una parte e le banche destinate alla comunicazione o alla diffusione dell'altra, si stende un ampio campo costituito dalle banche di dati che per scopo, quantità dei dati memorizzati o tipi di elaborazioni previste non possono dirsi destinate a soddisfare interessi personali nell'ambito della normale attività professionale o imprenditoriale.

Parimenti vi sono banche di dati personali che pur rientrando nella normale attività professionale o imprenditoriale dei soggetti che le hanno costituite richiedono pur tuttavia una certa disciplina; e ciò in quanto esse presentano una potenzialità lesiva del diritto alla riservatezza dell'individuo per il solo fatto della raccolta e della detenzione di dati da parte di un soggetto indipendentemente dalla possibile comunicazione dei dati stessi ad altri.

Rispetto a tali banche di dati personali permane un vuoto legislativo che costituisce al tempo stesso il limite, ma anche il pregio del disegno di legge. Difatti il gruppo di lavoro ha ritenuto che non fosse

[27] In ogni caso, se tale contrasto sussistesse, potrebbe essere ammessa una dichiarazione di esclusione ai sensi dell'art. 2, 2, a della Convenzione.

Inoltre l'art. 3, par. 2 della recente proposta di direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali prevede espressamente che le disposizioni della direttiva stessa non si applichino agli archivi:

a) detenuti da una persona fisica esclusivamente a fini privati e personali o

b) detenuti da associazioni senza scopo di lucro, in particolare a carattere politico, filosofico, religioso, culturale, sindacale, sportivo o ricreativo, nel quadro del loro scopo legittimo, a condizione che riguardino unicamente i membri e i corrispondenti dell'associazione che hanno consentito a figurarvi e che non siano comunicati a terzi.

Indubbiamente la nozione di « fine privato o personale » della proposta di direttiva europea è più ristretta di « scopo di soddisfare interessi personali, nell'ambito della propria vita privata e della propria attività professionale ed imprenditoriale » di cui al disegno di legge italiano. Entrambe, tuttavia, sono indici di una stessa tendenza, dettata dalla impossibilità di sottoporre alla disciplina legislativa quelle banche di dati personali necessari per l'esplicazione normale della propria attività.

possibile una normativa uniforme di una realtà così varia e continuamente mutevole; che una adeguata disciplina potesse in linea generale essere emanata solo per le banche di dati destinate alla comunicazione o alla diffusione; e che le altre potessero e dovessero essere regolate da distinte e apposite normative.

La disciplina delle banche di dati personali assume così un aspetto più complesso e articolato e rispetto ad essa il disegno di legge costituisce non l'unico, ma il primo dei possibili interventi legislativi.

4. I LIMITI DELLA LIBERTÀ INFORMATICA.

Principio fondamentale della nuova normativa è, come abbiamo visto, quello della libertà informatica, della libertà, cioè, di adoperare i mezzi informatici per le proprie personali esigenze senza vincoli ingiustificati.

Tuttavia anche alla libertà informatica e alle raccolte di dati destinate ad un uso privato possono essere imposti limiti di carattere generale. Tali limiti sono previsti nell'art. 3 del disegno di legge che vieta: *a*) l'inserimento in banche ad elaborazione informatica di dati raccolti fraudolentemente, con violenza o per scopi illeciti; *b*) la formazione di banche di dati personali ad opera di una pubblica amministrazione o di un ente pubblico per scopi diversi dall'adempimento delle funzioni loro proprie; *c*) l'elaborazione informatica dei dati cosiddetti sensibili (e cioè dei dati concernenti l'origine razziale, la fede religiosa, le opinioni politiche, l'appartenenza a partiti, sindacati, associazioni ed organizzazioni) se non su iniziativa o con il consenso espresso dell'interessato ovvero nel legittimo esercizio dell'attività giornalistica; *d*) l'elaborazione informatica dei dati concernenti le condizioni sanitarie, le anomalie fisiche o psichiche, l'uso di sostanze alcooliche o intossicanti, i comportamenti e le caratteristiche sessuali, se non da parte di determinati soggetti (e, cioè, gli esercenti le professioni sanitarie, gli organismi sanitari pubblici o privati, le imprese di assicurazione e gli enti previdenziali) ovvero con il consenso dell'interessato[28].

I dati sensibili sono stati individuati dalle varie normative europee in un modo abbastanza uniforme. In particolare l'art. 17 della recen-

[28] I cosidetti « dati sensibili » sono quei dati che hanno una particolare capacità di incidere sulla riservatezza dei singoli individui e di determinare discriminazioni sociali particolarmente odiose.

Sono state proposte in dottrina varie classificazioni dei dati sensibili come quella del tedesco HENCKEL, dello statunitense CAMBER e del norvegese BING. Il Italia RODOTÀ ha proposto di distinguere le informazioni in: *a*) informazioni obiettivamente neutre, la cui conoscenza, cioè. non può in alcun modo arrecare pregiudizio alla persona; *b*) informazioni che l'interessato potrebbe volere tenere riservate, ma la cui divulgazione è resa opportuna da finalità sociali (come quelle riguardanti il reddito imponibile); *c*) informazioni la cui diffusione non è desiderata dall'interessato e non è socialmente necessaria (come quelle sulle opinioni politiche o religiose). Quest'ultime costituiscono i dati di maggiore sensibilità o, come si esprimono alcuni autori, il « nucleo duro della riservatezza ».

te proposta di direttiva della Commissione della Comunità europea enumera le seguenti categorie:

a) origine razziale (ivi comprese le informazioni sul colore della pelle);

b) opinioni politiche, comunicazioni religiose e filosofiche (ivi compresa l'informazione secondo la quale una persona non ha convinzioni religiose) e informazioni sulle attività della persona interessata connesse a convinzioni politiche, religiose o filosofiche;

c) informazioni sull'adesione a sindacati;

d) informazioni riguardanti la salute della persona interessata (ivi comprese le informazioni sullo stato fisico o mentale passato, presente e futuro della persona interessata e le informazioni sull'abuso di droghe e di alcool);

e) le informazioni concernenti la vita sessuale.

Il nuovo disegno di legge distingue i dati sanitari dagli altri dati sensibili; subordina la liceità della raccolta al consenso dell'interessato; ammette il trattamento informatico dei dati sanitari senza il consenso dell'interessato soltanto da parte di sanitari o di imprese assicurative e previdenziali; consente l'elaborazione informatica degli altri dati sensibili soltanto se acquisiti nel legittimo esercizio dell'attività giornalistica.

La disciplina di cui all'art. 3 del nuovo disegno di legge trova il suo precedente nell'art. 10 del vecchio disegno di legge Martinazzoli che era in origine così formulato: « (Raccolta di dati particolari). I dati concernenti l'origine razziale, la fede religiosa, le opinioni politiche, l'appartenenza a partiti, sindacati, associazioni ed organizzazioni possono essere assoggettati ad elaborazione informatica soltanto con il consenso espresso dell'interessato ».

La norma così formulata era stata ritenuta da alcuni insufficiente e da altri eccessiva. Insufficiente perché subordinava la liceità della raccolta di tali dati al consenso dell'interessato, che è molto spesso apparente e del tutto necessitato. Il vietare la raccolta di dati personali se non con il consenso dell'interessato significa infatti considerare lecita la raccolta di qualsiasi tipo di informazione sui soggetti più deboli.

La norma era inoltre eccessiva, in quanto il divieto di raccolta di dati, anche se particolarmente sensibili, può costituire un grave ostacolo per la libertà di stampa e, più in generale, di informazione, per la ricerca scientifica, politica o sociologica. Poteva inoltre precludere l'uso dell'elaboratore a favore di una minoranza etnica o di gruppi di « diversi »[29].

[29] In base all'originaria formulazione dell'art. 10 i partiti politici, i sindacati, la Chiesa e le altre associazioni religiose non avrebbero potuto avvalersi di un elaboratore per automatizzare le liste dei propri iscritti; ed i giornali non avrebbero potuto memoriz-

In realtà la disciplina e la nozione stessa di dati sensibili sono in contrasto con il principio, ormai generalmente acquisito, che nessun tipo di dato è, in assoluto, contrario alla riservatezza dell'individuo, ma soltanto in relazione all'uso che si faccia del dato stesso. Come si legge nella proposta di direttiva del Consiglio, « il diritto alla vita privata può essere compromesso non tanto dal contenuto di un archivio, quanto dal contesto in cui si opera un trattamento di dati personali »[30].

Una disciplina generale dei dati sensibili risulta quindi necessariamente insufficiente da un lato e eccessiva dall'altro. Sarebbe stato quindi opportuno da una parte prevedere espressamente, così come è previsto nella proposta di direttiva, che il consenso dell'interessato deve essere libero, esplicito e scritto e i casi in cui il consenso dell'interessato deve presumersi.

Dall'altra parte sarebbe stato opportuno prevedere anche la possibilità di una particolare autorizzazione per la raccolta di dati sensibili anche senza il consenso dell'interessato qualora particolari esigenze lo richiedano.

Il regime autorizzatorio, permetterebbe di valutare in concreto l'effettiva pericolosità della banca di dati sensibili e la natura dei fini perseguiti. La raccolta di informazioni sulla salute potrebbe, ad esempio, essere autorizzata per fini scientifici o di ricerca, ma non per finalità commerciali; ovvero potrebbe essere autorizzata anche per questi fini mediante la predisposizione delle misure necessarie per impedire i possibili abusi.

zare, ad esempio, il nome del segretario del partito della Democrazia Cristiana o di un altro partito qualsiasi.

A seguito delle critiche sollevate, all'art. 10 erano state aggiunte le parole: « O se acquisiti nel legittimo esercizio dell'attività giornalistica ». Corrispondente integrazione era stata apportata all'ultimo comma dell'art. 13 cui sono state aggiunte le parole: « O il dato sia stato raccolto nei modi previsti dall'art. 10 ». Con tali aggiunte si prevedeva specificamente che la disciplina del progetto di legge non intendeva limitare il legittimo esercizio del diritto di cronaca (MIRABELLI G., *Osservazioni e rilievi allo schema di d.d.l. sulle banche di dati*, in *I quaderni della Giustizia*, 1983, p. 27.

Lo stesso autore aggiungeva: « Sembra... evidente che la raccolta dei dati comunicati da ogni iscritto da parte dell'associazione medesima deve ritenersi consentita a seguito della stessa domanda di iscrizione; ma con questa non deve ritenersi consentita la ulteriore elaborazione ai fini di comunicazione a terzi, che va invece assoggettata all'espresso consenso dell'interessato ».

In tale modo, tuttavia, si operava una distinzione che non trovava alcun riscontro nel testo della legge di ipotizzava una figura di consenso tacito che rendeva ancor più illusoria la tutela.

Opportunamente ha affermato al riguardo Stefano Rodotà: « Dans cette matière, le problème du consentement tacite est un pas très dangereux que je ne voudrais jamais franchir ».

[30] Nella conferenza del Consiglio d'Europa tenuta a Roma nel 1983 Spiros Simitis ha affermato: « Tout le monde est d'accord lorsq'il s'agit d'interdire la collecte de donnés rélevant l'origine raciale, les convictions religieuses, les opinions politiques. Mais, en vérité, ceci est une fiction parce que tout dépend du contexte. Il est évident que les syndicats auront des informations sur l'appartenance d'une personee au syndacat. Il en est de même des partis politiques et l'on ne saurait interdire à l'Eglise catholique de disposer d'un fichier des catholiques. Comme nous avons souligné la nécessité de nous limiter à des conflits précis, il faut donc éviter des régles aussi générales ».

Discipline autorizzatorie o in deroga per quanto riguarda i dati sensibili sono previste nella normativa svedese del 1982 e nella normativa francese.

La normativa svedese del 1982 ha, come abbiamo visto, sostituito il regime dell'autorizzazione, previsto dalla precedente legge del 1973, con la licenza. Tuttavia la norma continua a richiedere l'autorizzazione nei casi in cui l'archivio sia destinato a contenere dati particolarmente sensibili.

L'art. 31 della legge francese, invece, dispone: « È vietato mettere e conservare in una memoria elettronica, salvo assenso espresso dell'interessato, nominativi che, direttamente o indirettamente, rivelino le origini razziali o le opinioni politiche, filosofiche o religiose o l'aderenza sindacale delle persone.

Tuttavia le chiese ed i gruppi a carattere religioso, filosofico, politico o sindacale possono tenere la registrazione in forma automatizzata dei loro membri e dei loro corrispondenti. Nessun controllo può essere esercitato nei loro riguardi.

Per motivi di interesse pubblico può essere fatta deroga al divieto di cui sopra su proposta o parere conforme della Commissione con decreto sentito il Consiglio di Stato ».

5. Il garante della libertà informatica.

L'art. 9 del disegno di legge prevede l'istituzione di un organo di garanzia per assicurare il controllo dell'attuazione della legge stessa; e l'art. 10 ne indica i compiti.

Il disegno di legge Martinazzoli, invece, prevedeva non già l'istituzione di un Garante, ma quella di un Ufficio di controllo delle banche di dati presso la Presidenza del Consiglio dei Ministri.

Sia l'istituzione dell'Ufficio di controllo, sia l'istituzione del Garante, sono state fatte in adempimento della Convenzione europea e in conformità della grandissima parte delle normative in materia. Tuttavia la distinzione tra Garante e Ufficio di controllo non è semplicemente terminologica, ma corrisponde ad una diversa concezione dei compiti e della natura dei due organi.

Secondo una prima concezione, infatti, l'Ufficio di controllo dovrebbe essere un organo tecnico e svolgere una attività di carattere prevalentemente sanzionatorio e repressivo. In sostanza l'Ufficio dovrebbe accertare le eventuali violazioni della legge ed applicare le relative sanzioni.

Il disegno di legge Martinazzoli prevedeva, infatti, la composizione dell'ufficio da parte di magistrati e di personale della Pubblica Amministrazione nominati dal Presidente del Consiglio dei Ministri con l'ausilio di esperti (art. 5), la collocazione presso la Presidenza del Consiglio dei Ministri e, comunque, l'inquadramento di esso nell'ambito della Pubblica Amministrazione. All'Ufficio era, quindi, attribuito un insieme di poteri sanzionatori e repressivi compreso quel-

lo, più grave di tutti, di ordinare l'immediata cessazione dell'attività della banca di dati qualora fosse stato accertato che la banca stessa veniva esercitata senza la notifica ovvero in difformità del contenuto della stessa o, comunque, in violazione delle disposizioni di legge (art. 6 n. 7).

La configurazione dell'Ufficio di controllo, quale risultava dal disegno di legge governativo, era stata oggetto di numerose critiche e, come aveva notato lo stesso Mirabelli, era stata accolta con sorpresa dagli esperti del Consiglio d'Europa in occasione del convegno tenuto a Roma nel 1983[31].

Era stata soprattutto contestata la collocazione dell'Ufficio presso la Presidenza del Consiglio dei Ministri e, comunque, l'inquadramento di esso nell'ambito della Pubblica Amministrazione; ed era stata sottolineata l'esigenza di una maggiore indipendenza dell'Ufficio medesimo.

Inoltre i poteri attribuiti all'Ufficio erano apparsi per alcuni aspetti eccessivi. In particolare le associazioni imprenditoriali avevano sollevato dubbi di legittimità costituzionale della norma che prevedeva il potere dell'Ufficio di ordinare la cessazione della banca di dati; avevano fatto presente che il provvedimento, se fosse stato assunto illegittimamente, avrebbe potuto produrre danni economici ingentissimi alle imprese interessate; e avevano auspicato che all'Ufficio di controllo venisse attribuito un limitato potere di denuncia all'autorità giudiziaria, eventualmente con la previsione della competenza esclusiva di un organo giudiziario specializzato.

A queste critiche era stato significativamente risposto che il potere sanzionatorio costituiva un punto centrale della normativa e che l'unico efficace deterrente nei confronti dell'inosservanza della legge era, appunto, la previsione di un intervento immediato che facesse cessare la violazione[32].

A questa concezione dell'Ufficio di controllo si contrappone, peraltro, una diversa concezione che vede in esso non tanto un organo tecnico destinato a svolgere un controllo di carattere repressivo e sanzionatorio, quanto piuttosto un organo rappresentativo e di promozione. Un organo che non si limiti ad accertare le violazioni compiute, ma tenda piuttosto a farsi interprete delle esigenze delle imprese e di

[31] MIRABELLI G., *Osservazioni e rilievi allo schema di DDL sulle banche di dati*, in *Quaderni della Giustizia*, n. 31 p. 25; gli atti della conferenza di Roma degli esperti del Consiglio d'Europa sono stati raccolti e pubblicati a cura della Camera dei Deputati.

[32] MIRABELLI G., *Osservazioni e rilievi allo schema di DDL sulle banche di dati*, in *Quaderni della Giustizia*, n. 31 p. 25. Per quanto riguarda la composizione occorre osservare che alcune normative come ad esempio quella svedese, quella francese e quella austriaca prevedono una pluralità di membri; altre come quella tedesca o quella britannica un organo monocratico (il delegato federale tedesco e il Registrar britannico). Tutte peraltro assicurano una vasta rappresentatività degli organi collegiali, l'indipendenza dell'Ufficio da parte del Governo e il suo stretto collegamento con il Parlamento o con il Capo dello Stato.

tutti i cittadini nel settore dell'automazione, controlli la corrispondenza della legge a tali esigenze e promuova le necessarie modifiche normative.

La maggioranza delle normative europee si ispira a questa seconda concezione: e ciò spiega la diversa composizione dell'Ufficio rispetto al disegno di legge Martinazzoli e i diversi poteri ad esso attribuiti[33].

Il secondo disegno di legge italiano ha previsto il Garante per l'informazione informatizzata, un organo di controllo del tutto indipen-

[33] Ad esempio, nella normativa svedese (Datalag), l'Ispettorato per i dati (Datainspektionen) è composto di 11 membri (1 magistrato in qualità di presidente, 4 parlamentari, 3 rappresentanti del mondo del lavoro, 1 informatico, 1 funzionario amministrativo, 1 medico) provenienti dalle più diverse categorie. Oltre al compito di controllare l'osservanza della legge, l'Ispettorato svolge un'attività di informazione, di consulenza, di studio degli effetti delle nuove tecnologie, di partecipazione nelle sedi internazionali alla discussione su materie di propria competenza.

In particolare l'ispettorato dei dati è tenuto a presentare annualmente un rapporto al Governo sull'attività svolta ed un rapporto al Parlamento contenente le risposte date nel corso dell'anno ai quesiti posti dai parlamentari e le eventuali proposte di modifiche normative alla luce delle esperienze acquisite durante l'anno.

Anche per la normativa tedesca il delegato federale per la protezione dei dati personali può formulare raccomandazioni per il miglioramento della protezione dei dati ed, in modo particolare, può consigliare il Governo federale e i singoli ministri nonché le altre autorità in questioni relative alla protezione dei dati (art. 19, 1).

Su richiesta del Bundestag o del Governo federale, il delegato federale deve rilasciare pareri e predisporre relazioni. Inoltre egli redige per il Bundestag con regolarità annuale e a partire dal 1° gennaio 1979 una relazione sull'attività svolta. Su richiesta del Bundestag, della Commissione per le interpellanze del Bundestag o del Governo federale può approfondire questioni che si riferiscono ad affari e ad atti che riguardano direttamente il settore di sua competenza. Il delegato si può rivolgere al Bundestag in qualsiasi momento.

La normativa austriaca prevede, invece, una Commissione per le protezione dei dati ed un Consiglio per la tutela dei dati. La Commissione per la protezione dei dati, oltre all'espletamento dell'attività di controllo, ha il compito di redigere ogni due anni un rapporto sull'attività svolta e sulle esperienze raccolte e le trasmette al capo del Governo. Il Capo del Governo presenta tale rapporto al Parlamento (Nationalrat) unitamente ad un parere del Governo e del Consiglio per la tutela dei dati e a un prospetto sullo sviluppo dell'elaborazione e della tutela dei dati all'estero e con le raccomandazioni del caso. Se il rapporto si riferisce all'elaborazione di dati effettuata nell'ambito dei Länder il Capo del Governo lo trasmette a questi ultimi, unitamente al parere del Consiglio per la tutela dei dati (art. 46).

Il Consiglio per la tutela dei dati, oltre ad altre competenze, ha anche il compito di:

1) richiedere informazioni e rapporti agli organi competenti sui problemi sollevati dalla tutela dei dati nella sfera pubblica;

2) osservare gli effetti della circolazione dei dati sulla salvaguardia degli interessi meritevoli di tutela, in particolare sul rispetto della vita privata e familiare, e allargare i risultati di tali osservazioni al rapporto della Commissione per la protezione dei dati;

3) manifestare sollecitazioni o suggerimenti per il miglioramento della protezione dei dati che appaiono necessari in seguito allo sviluppo della circolazione dei dati a tutela dei diritti costituzionalmente garantiti, al Governo Federale e a quelli locali, così come esprimere anche la propria opinione in merito al coordinamento di questi ultimi con gli organi legislativi;

4) promuovere discussioni su problemi di significato fondamentale per la protezione dei dati su richiesta di uno dei rappresentanti dei partiti politici facenti parte del Consiglio;

5) emanare il proprio regolamento di servizio (art. 42).

Anche per il Data Protection Bill britannico il Registrar è tenuto a presentare a ciascuna Camera del Parlamento una relazione annuale sull'attività svolta e potrà, di volta in volta, presentare a ciascuna Camera altre relazioni ogniqualvolta lo riterrà opportuno.

Il Registrar può anche far circolare, nelle forme e nei modi ritenuti adeguati, le informazioni e le proposte che egli considererà opportuno rendere di pubblica ragione concernenti l'attuazione della legge e le altre questioni che rientrano nel quadro delle sue attribuzioni (art. 33).

dente dal Governo e dalla Pubblica Amministrazione e ispirato alla figura del Garante dell'editoria istituito con la legge 5 agosto 1981, n. 416. Entrambi, infatti, sono organi monocratici, nominati da parte dei Presidenti delle due Camere, dotati di autonomia amministrativa e contabile, nonché di un ufficio senza ruolo di personale (artt. 9 e 11). La figura del Garante ha perso il carattere autoritario e repressivo propri dell'Ufficio di controllo del primo disegno di legge e ha assunto piuttosto la funzione di promovimento e di garanzia della libertà informatica.

In particolare il Garante ha il compito di curare la diffusione tra il pubblico della conoscenza della normativa contenuta nella legge, delle finalità della stessa e dell'attività svolta dal Garante (art. 10 n. 8), di presentare al Parlamento una relazione biennale sullo stato di attuazione della legge (art. 10 n. 9), di segnalare al Governo l'opportunità di provvedimenti legislativi o regolamentari richiesti dall'evoluzione delle situazioni disciplinate dalla legge (art. 10 n. 10).

Al Garante sono stati attribuiti, inoltre, il compito di formare il registro generale delle banche di dati personali (art. 10 n. 1) e il potere di controllo sulle banche notificate (art. 10 n. 2).

L'espletamento di tali compiti, tuttavia, non prevede l'attribuzione di poteri coercitivi o repressivi, ma di poteri diversi come quello di segnalare al responsabile le modificazioni opportune al fine di rendere la banca conforme a legge (art. 10 n. 3), di ricevere le segnalazioni degli interessati relative all'osservanza della legge, di controllarne la fondatezza e di indicare al responsabile le misure opportune (art. 10 n. 4), di denunciare al pubblico ministero i fatti configurabili come reato perseguibile di ufficio (art. 10 n. 5).

Peraltro la facoltà del Garante di richiedere l'accesso alla banca o informazioni sul funzionamento come mezzo per esercitare la vigilanza (art. 10 comma 2) non è tutelata da alcuna specifica sanzione ed è pertanto applicabile la generale disciplina della inosservanza dei provvedimenti della pubblica autorità.

Infine è attribuito al Garante il potere di emettere alcuni particolari provvedimenti di divieto o di autorizzazione per la tutela di specifici pubblici interessi (art. 10 n. 6 e 7) come, ad esempio, il potere di vietare la diffusione di taluno dei dati relativi a singoli soggetti o a categorie di soggetti per motivi di ordine pubblico o quando la diffusione sia in contrasto con rilevanti interessi della collettività (art. 15 u.c.), il potere di autorizzare la comunicazione di dati da una pubblica amministrazione ad un'altra, quando la comunicazione soddisfi un rilevante pubblico interesse (art. 16), il potere di vietare il trasferimento di dati personali fuori del territorio nazionale ove il Garante accerti che l'ordinamento del Paese nel territorio del quale o tramite il territorio del quale ha luogo il trasferimento contiene norme in contrasto con la legge (art. 20 u.c.).

In sostanza il Garante tende più che a controllare le banche di dati, a promuoverne l'attività nella giusta direzione; più che a disporre ciò che devono fare, a invitarle a farlo; più che a sanzionare i comportamenti illeciti, a denunziarli alle autorità competenti.

In tal modo il Garante ha perso il carattere autoritario e repressivo del primo disegno di legge ed è divenuto un organo di promovimento e di garanzia della libertà informatica.

La nuova natura ed i diversi poteri attribuiti al Garante hanno reso inutile la complessa normativa contenuta nel disegno di legge Martinazzoli circa la tutela amministrativa e giurisdizionale dei cittadini nei confronti dei provvedimenti o, comunque, dell'attività dell'Ufficio di controllo[34].

6. Il diritto di accesso.

Il disegno di legge Martinazzoli prevedeva una serie di diritti e di obblighi e in particolare: *a*) l'obbligo del responsabile di notificare l'esistenza della banca di dati personali all'Ufficio di controllo; *b*) l'obbligo di comunicare l'inserimento nella banca di dati personali al soggetto al quale i dati si riferiscono (artt. 13 e 14) nonché l'obbligo di certificare al titolare del dato le comunicazioni dei dati fatte a terzi con specificazione del tempo, delle modalità e dello scopo della comunicazione (art. 14 n. 6).

L'imposizione di un indiscriminato obbligo di comunicazione dell'inserimento di ogni dato personale, di tutte le loro modifiche e delle comunicazioni di essi a terzi aveva suscitato numerose critiche.

Tale imposizione, infatti, costituiva un onere vasto e gravoso che non trovava riscontro nelle legislazioni degli altri Paesi Europei[35].

[34] In particolare era previsto che avverso gli atti dell'Ufficio potesse proporsi ricorso al Tribunale amministrativo regionale di Roma (art. 7); e che indipendentemente dalla proposizione e dall'esito del ricorso all'Ufficio di controllo, l'interessato potesse domandare all'Autorità giudiziaria ordinaria, anche in deroga al divieto di cui all'art. 4 della legge 20 marzo 1865, n. 2248 allegato E, la condanna dei soggetti o degli organi di cui al n. 1 della legge al compimento delle operazioni dovute e al risarcimento del danno, nonché i provvedimenti cautelari previsti dalle leggi processuali (art. 22, comma 2).

Competente a giudicare su tali domande era il Tribunale del luogo dove aveva sede la Corte di Appello nel cui distretto si trovava il giudice che sarebbe stato competente secondo le norme ordinarie (art. 22, comma 3).

La possibilità di adire, anche in via concorrente, l'Autorità giudiziaria ordinaria era coerente con la costruzione del diritto di accesso quale vero e proprio diritto soggettivo. Tuttavia, era stato giustamente osservato, la prevista possibilità di ricorso a due distinti organi giudiziari avrebbe potuto dar luogo a notevoli difficoltà (Catania N., *Dossier Privacy*, Edizioni Sarin, Roma, 1983, p. 56); difficoltà venute meno con il nuovo disegno di legge volto soprattutto a promuovere l'attività informatica e a risolvere preventivamente le controversie.

[35] Infatti sia in Svezia, sia in Francia, sia nel Regno Unito non è previsto alcun preventivo e indiscriminato obbligo di comunicazione, ma solo un diritto di accesso, il diritto, cioè, dell'interessato di conoscere la inclusione di dati che lo riguardano in raccolte ad elaborazione informatica e di controllare l'esattezza e l'attualità del dato.

Anche in Germania vi è un obbligo non già di comunicazione ai singoli interessati, ma solo di una pubblicità relativa ai dati memorizzati (art. 12 legge 27 gennaio 1977); l'obbligo di fornire informazioni alle persone interessate sui dati memorizzati che le riguardano è subordinata ad una richiesta scritta ed al pagamento dei diritti (art. 13 legge 27 gennaio 1977).

In particolare dispone l'art. 13:

Informazioni agli interessati.

1) Su richiesta dell'interessato devono essere fornite informazioni sui dati memorizzati che lo concernono. Nella richiesta deve essere indicata, in dettaglio, la natura dei dati personali sui quali deve essere fornita l'informa-

In sostanza mentre nel disegno di legge Martinazzoli il responsabile della banca di dati doveva comunicare all'interessato l'inserzione dei dati che lo riguardavano e le modifiche dei dati inseriti, nelle altre legislazioni, invece, il responsabile della banca non aveva l'obbligo di comunicare i dati che riguardano un determinato individuo, ma solo di adottare i provvedimenti necessari per potere comunicare tali dati qualora la persona interessata li richiedesse. La richiesta doveva, in genere, essere effettuata in forma scritta e — secondo alcune normative — non poteva essere reiterata se non ad intervalli di tempo ragionevoli[36]; era inoltre, subordinata al pagamento delle spese sia pure nella misura indicata dall'autorità di controllo.

La differenza era notevole ed implicava un ben diverso onere economico per le imprese. In Germania è stato calcolato che la normativa sulle banche dei dati comporta un onere economico pari all'1% o al 2% delle spese globali per l'elaborazione dei dati[37]; la disciplina del disegno di legge Martinazzoli avrebbe comportato un onere sicu-

zione. La procedura e in particolare le modalità di trasmissione di tali informazioni vengono stabilite secondo il suo prudente apprezzamento dallo stesso ufficio comunicante.

2) Il comma 1 non si applica nei casi previsti dall'art. 12, comma 2, nn. 1 e 2.

3) Le informazioni non vengono rilasciate se:

1. le informazioni stesse possono mettere in pericolo il corretto adempimento dei compiti che rientrano nella competenza della unità di memorizzazione;

2. le informazioni possono mettere in pericolo la pubblica sicurezza o l'ordine pubblico o comunque essere di pregiudizio alla Repubblica federale o a un Land;

3. i dati personali o le modalità della loro memorizzazione devono rimanere segreti in base ad una disposizione di legge o per la loro stessa natura, e particolarmente per i legittimi e prevalenti interessi di una terza persona;

4. le informazioni si riferiscono alla trasmissione di dati personali alle autorità indicate nell'art. 12, comma 2, n. 1.

4) Il rilascio delle informazioni avviene dietro corresponsione di diritti. Il governo federale è autorizzato, tramite provvedimento delegato soggetto alla approvazione del Bundesrat a stabilire in dettaglio le fattispecie nelle quali è prevista la corresponsione dei diritti e l'ammontare dei diritti stessi, nonché a prevedere eccezioni all'obbligo di corresponsione. I diritti possono essere percepiti solamente per la copertura delle spese amministrative direttamente connesse ad atti di ufficio di questa natura. Le eccezioni all'obbligo di corresponsione dei diritti sono consentite particolarmente nei casi in cui, per speciali circostanze, si può fondatamente ritenere che i dati personali sono stati memorizzati in modo inesatto o che la loro memorizzazione era inammissibile, o nei casi in cui le informazioni hanno portato alla correzione o alla cancellazione di dati personali memorizzati. Per il resto si applica la legge sulle spese nel procedimento amministrativo.

Discipline analoghe sono contenute nella legislazione canadese (art. 12 e 13 del Canadian Human Rights Act del 2 giugno 1977), danese (art. 13 della legge 8 giugno 1978, n. 294 sui registri tenuti dall'amministrazione pubblica), norvegese (art. 7 della legge 9 giugno 1978, n. 48 sui registri di dati personali), austriaca (art. 11 della Datenschutzgesetz - DSG - del 18 ottobre 1978, n. 565), lussemburghese (artt. 19 e 20 della legge 31 marzo 1979 riguardante l'utilizzazione dei dati nominativi nei sistemi informatici), islandese (artt. 10 e 11 della legge n. 63/1981 sulla registrazione sistematica di dati personali), israeliana (art. 13 della legge sulla protezione privata n. 5741/1981) e svizzera (art. 4.3 delle direttive del Consiglio Federale svizzero emesse il 16 marzo 1981 ed applicabili al trattamento dei dati personali nell'amministrazione federale).

[36] V. in particolare la disciplina contenuta nel Data Bill Protection britannico.

[37] I dati sono riportati da Losano M.G., *La legislazione tedesca sulla protezione dei dati individuali*, in *Banche dati e tutela della persona*, Camera dei Deputati, 2ª ed. Roma, 1983, — per alcuni, peraltro, i costi per la protezione dei dati personali sarebbero ancora più elevati.

ramente maggiore e quindi tale da porre l'industria italiana in situazione di sfavore nell'ambito del commercio internazionale[38].

Il nuovo disegno di legge ha sostituito l'indiscriminato obbligo di comunicazione con il diritto di accesso, ossia con un vero e proprio diritto soggettivo di accedere ai propri dati personali conservati in banche ad elaborazione informatica[39].

Si tratta di una nuova figura soggettiva, prevista dalla Convenzione di Strasburgo, che può avere un contenuto diverso a seconda delle varie normative.

Nel nuovo disegno di legge italiano la tutela prevede « l'attribuzione all'interessato della facoltà di ricevere dall'ufficio del Garante, con diretto accesso al sistema informatico di questo, informazioni intorno a banche di dati notificate che possono contenere dati personali che lo concernono e della facoltà di ottenere dal responsabile della banca l'attestazione dei dati inseriti, la cancellazione dei dati raccolti illegittimamente, eccedenti od obsoleti, l'aggiornamento, la rettificazione e, ove dimostri di avervi giustificato interesse, il completamento dei dati inseriti, nonché l'attestazione che le rettifiche sono portate a conoscenza di coloro cui è pervenuta comunicazione o diffusione del dato »[40].

Il disegno di legge riconosce la titolarità del diritto di accesso a ognuno (art. 12) ossia, in base al disposto di cui all'art. 1, lett. *e*), a ogni interessato, persona fisica o giuridica o ente di fatto o altra figura soggettiva cui si riferiscono i dati inseriti nella banca.

Il termine interessato ricorre in vari articoli della legge (artt. 3, 7, 10 n. 4, 23), ma, soprattutto, è il requisito soggettivo per l'attribuzione della titolarità del diritto di accesso (artt. 12, 13), del diritto di vietare la comunicazione e la diffusione dei dati (artt. 14, 15, 16, 17, 18) e, più in generale, per agire in giudizio per il risarcimento nei confronti di chi in violazione della legge abbia procurato all'interessato un danno ingiusto (*ex* artt. 2043 cod. civ. e 100 cod. proc. civ.).

Secondo il disegno di legge, pertanto, chiunque, sia esso persona fisica o giuridica o impresa o qualsiasi altra figura soggettiva può esercitare i diritti previsti dalla legge e, in mancanza, può agire per il risarcimento del danno quando si tratta di dati che lo riguardino ossia che ne possano permettere l'identificazione.

Indubbiamente l'estensione della protezione ai dati delle persone giuridiche e delle altre figure soggettive diverse dalle persone fisiche

[38] La disciplina risulta tanto più onerosa qualora si consideri quanto poco il diritto di accesso sia stato esercitato negli Stati che lo hanno previsto. Particolarmente interessante è al riguardo l'esperienza degli Stati Uniti d'America. L'art. 3 lett. *d*) del Privacy Act prevede, infatti, un diritto di accesso dei cittadini statunitensi ai dati personali posseduti dal Governo Federale. La Commissione di studio sulla protezione della vita privata ha rilevato una tale passività degli utenti al riguardo (negli anni 1977-1978 su 4.588 rifiuti di comunicazione sono stati presentati soltanto 141 ricorsi giurisdizionali) da auspicare l'istituzione di una Commissione federale dotata di ampi poteri di controllo anche preventivo.

[39] Dalla relazione del gruppo di studio del Ministero di Grazia e Giustizia.

[40] Dalla relazione del gruppo di studio del Ministero di Grazia e Giustizia.

costituisce un punto di merito del disegno di legge rispetto a quelle legislazioni che limitano la tutela alle sole persone fisiche.

L'estensione della tutela a figure soggettive diverse dalla persona fisica, peraltro, è un argomento vivamente dibattuto e sia la Convenzione Europea, sia la Direttiva dell'O.C.S.E. hanno evitato di prendere posizione al riguardo, ma si sono limitate ad ammettere che ogni Paese aderente possa estendere la tutela ad associazioni, fondazioni, società ed enti aventi o meno personalità giuridica.

L'estensione della tutela era prevista anche nel disegno di legge Martinazzoli; essa, tuttavia, aveva incontrato notevoli opposizioni, in ispecie da parte delle associazioni imprenditoriali. In particolare era stato osservato che si trattava di una tutela che non interessava le società commerciali ed, anzi, ne pregiudicava le attività.

L'argomento sul quale è costantemente fondata la tesi della esclusione e che fu magistralmente esposto nella « Risoluzione politica sulla legislazione della privacy, sulla tutela dei dati e sulle persone giuridiche », adottata dalla Camera di commercio internazionale nel 1984, consiste nel rilievo che ogni impresa ha interesse ad acquisire e mantenere informazioni su altre imprese, ma verrebbe pregiudicata se alle altre imprese, i cui dati sono stati raccolti ed assoggettati ad elaborazione informatica, venisse riconosciuto il diritto di conoscere l'esistenza ed il contenuto della raccolta, giacché ne verrebbe menomata la libertà di concorrenza.

L'argomento concerne, invero, le imprese in generale e non le sole società, ed il riferimento alle persone giuridiche è fondato, forse, sulla circostanza che in altri ordinamenti all'impresa, in quanto tale, è riconosciuta una soggettività giuridica, che è ignota al diritto italiano.

Appare, però, evidente che l'interesse che con l'esclusione si intende salvaguardare è quello stesso interesse all'informazione per scopi personali che nel secondo disegno di legge Mirabelli viene considerato prevalente sul generico interesse alla riservatezza e soltanto assoggettabile a limiti, ove si ponga in conflitto con specifici interessi della persona.

Nei confronti del sistema proposto nel disegno di legge nel quale viene riconosciuta la piena libertà di raccolta di dati per scopi personali e si riconoscono come scopi personali anche quelli inerenti all'attività imprenditoriale, estendendo la nozione di scopo personale agli scopi perseguiti in attività che vengano svolte « unitamente » ad altri soggetti (art. 2, comma 2), l'argomento che sorregge la tesi dell'esclusione viene totalmente a cadere, in quanto una facoltà di accesso di imprenditori concorrenti rimane esclusa.

Se, per converso, i soggetti diversi dalle persone fisiche venissero esclusi dalla tutela, a questi verrebbero preclusi sia la facoltà di ottenere il controllo, sia il diritto di accesso alle raccolte che diffondono dati che li riguardano; tali soggetti, imprenditori o meno, non potrebbero pretendere di conoscere i dati raccolti per la diffusione, né ottenerne l'aggiornamento, la rettifica o l'eliminazione per obsolescenza, né potrebbero esercitare le facoltà di limitazione e divieto che ad ogni interessato vengono riconosciute (art. 15).

Nel sistema proposto l'esclusione delle persone giuridiche e degli enti diversi dalle persone fisiche dall'ambito della tutela non soltanto risulterebbe, dunque, ingiustificata, ma impedirebbe la tutela di interessi che ne sono meritevoli.

Per queste considerazioni il gruppo ha ritenuto di mantenere l'inclusione, tra i soggetti tutelati, di ogni ente, avente o meno personalità giuridica, e conseguentemente sia delle imprese individuali che delle imprese collettive.

Tutte queste entità vengono incluse, quindi, nella figura dell'« interessato », definita dalla lettera e dell'art. 1.

Non è dubbio, pertanto, che il diritto di accesso spetti non soltanto alle persone fisiche, ma anche a figure soggettive diverse come le associazioni, i sindacati o le persone giuridiche che possono agire per la tutela della riservatezza dei dati loro relativi. Vi è in questi casi una perfetta coincidenza tra i dati oggetto della tutela e la titolarità del diritto di accesso.

È dubbio, invece, se una persona giuridica o un'associazione non riconosciuta, possa agire per la tutela dei dati relativi ai propri membri: se, ad esempio, possa essere riconosciuto il diritto dei sindacati di accedere alle informazioni raccolte sui dipendenti al fine di controllare se vi siano stati abusi da parte del datore di lavoro nella raccolta di taluni tipi di informazioni.

Va inoltre tenuto presente che la norma deve essere coordinata con quelle disposizioni di leggi speciali che riconoscono il diritto di accesso anche nei riguardi di dati personali altrui quando speciali cause lo giustifichino ovvero nei riguardi di dati anonimi o collettivi o pubblici. In materia tributaria, ad esempio, potrebbe essere riconosciuto a ciascun cittadino il diritto di prendere visione non solo del proprio, ma anche del dossier fiscale di qualsiasi altro cittadino.

A favore di un riconoscimento il più vasto possibile della titolarità del diritto di accesso sta la considerazione che anche la conoscenza di un dato altrui può costituire interesse da tutelare quando speciali cause lo giustifichino; che l'azione di raccolta di dati personali da parte dei pubblici poteri diventa, in mancanza di ogni possibilità di controllo, più oscura e meno democratica; che anche le raccolte di dati anonimi possono essere adoperate in modo gravemente lesivo dei diritti dei singoli; che, in sostanza, la possibilità di accesso ad ogni specie di dati, anche anonimi o collettivi, è alla base di una informazione e di una partecipazione democratica del cittadino alla vita politica.

In definitiva, quindi, il potere di controllo dell'individuo nei confronti dell'elaboratore va inteso nel senso più ampio possibile perché, come è stato detto incisivamente, non si tratta soltanto di fornire all'individuo un *habeas scriptum*, come mezzo di difesa contro l'elaboratore, ma di consegnargli quest'ultimo come mezzo di controllo e di partecipazione sociale[41].

[41] RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, p. 121.

7. Comunicazione e diffusione dei dati.

La lett. *f*) e la lett. *g*) dell'art. 1 del disegno di legge definiscono la comunicazione come il « dare conoscenza dei dati elaborati a soggetto determinato diverso dall'interessato » e la diffusione come il « dare conoscenza dei dati elaborati a soggetti indeterminati ».

Si tratta di definizioni che in termini molto simili ricorrono anche in leggi straniere, ma che nel disegno di legge italiano assumono un particolare significato. Il campo di applicazione della legge, infatti, è limitato, come abbiamo visto, alle banche di dati destinati ad essere diffusi o comunicati a terzi. La notificazione e il diritto di accesso riguardano soltanto le banche di dati destinate alla comunicazione o alla diffusione.

Peraltro l'adempimento dell'obbligo di notificazione e dell'obbligo corrispondente al diritto di accesso non comporta, di per sé, la facoltà di comunicazione o di diffusione dei dati. Tale facoltà, infatti, viene subordinata al consenso dell'interessato che può essere esplicito ossia reso attraverso un'espressa dichiarazione ovvero implicito ossia consistente in un comportamento al quale, secondo i criteri della diligenza e della buona fede, va attribuito il significato di consenso.

L'art. 14 indica inoltre quattro ipotesi in cui il consenso deve considerarsi implicito, presunto o comunque irrilevante: *a*) se il dato sia stato ottenuto dall'interessato e questi sia stato in grado di conoscere, usando la normale diligenza, che il dato sarebbe stato destinato alla comunicazione o alla diffusione (art. 14 n. 2); *b*) se il dato sia stato legittimamente tratto da pubblici registri o da atti o documenti conoscibili da chiunque (art. 14 n. 3); *c*) se l'inserimento del dato nella banca sia stato tempestivamente portato a conoscenza dell'interessato e questi non abbia prontamente dichiarato di vietarne, in tutto o in parte, la comunicazione o la diffusione o la comunicazione a determinate categorie di terzi (art. 14 n. 4); *d*) se la comunicazione o la diffusione sono compiute nel legittimo esercizio dell'attività giornalistica (art. 14 n. 5).

Si tratta di ipotesi evidentemente alternative tra loro e soggette alla possibilità di ulteriori divieti e di eccezioni.

Gli ulteriori divieti sono previsti dall'art. 15 che vieta in ogni caso la comunicazione e la diffusione dei dati per scopi diversi da quelli indicati nella notificazione, dei dati di cui sia stata disposta la cancellazione, dei dati conservati per un periodo di tempo superiore a quello necessario per l'attuazione dello scopo.

La norma, inoltre, prevede un potere di divieto di dati, altrimenti comunicabili o diffondibili, da parte dell'interessato e del Garante. Il primo può vietare la comunicazione o la diffusione di taluno dei dati che lo concernono, ancorché pertinenti allo scopo della raccolta, se dimostri di avervi un giustificato interesse; il secondo, invece, può vietare la diffusione dei dati relativi a singoli soggetti, o a categorie di soggetti, per motivi di ordine pubblico o quando la diffusione sia in contrasto con rilevanti interessi della collettività.

Le eccezioni sono, invece, previste nell'art. 19 per il quale la comunicazione e la diffusione dei dati sono comunque permesse: *a*) quando sia-

no richieste per scopi di studio, di ricerca, di statistica e simili e attuate in modo che non sia possibile l'identificazione dell'interessato ovvero l'identificazione richieda un eccessivo impiego di tempi e di mezzi; *b*) quando siano richieste per scopi concernenti la difesa dello Stato o l'accertamento di reati, con l'osservanza delle norme che regolano la materia.

Il disegno di legge, infine, prevede una speciale disciplina per la comunicazione e la diffusione di tre categorie di dati: i dati delle banche della Pubblica Amministrazione (art. 16), i dati sensibili (art. 17) e i dati sanitari (art. 18).

Precisamente dispone l'art. 16: « Comunicazione e diffusione di dati delle banche della Pubblica Amministrazione — Alle pubbliche amministrazioni è consentito diffondere o comunicare ad altra pubblica amministrazione o a privati i dati inseriti in una banca di dati ad elaborazione informatica soltanto quando la comunicazione o la diffusione sono previste da norme di legge o di regolamento; tuttavia il Garante può autorizzare la comunicazione di dati ad altra pubblica amministrazione, quando la comunicazione soddisfi un rilevante pubblico interesse ».

L'art. 17, prevede, invece che la comunicazione o la diffusione dei dati sensibili è ammessa soltanto con il consenso dell'interessato o nel legittimo esercizio delle attività giornalistiche.

Infine l'art. 18 regola la comunicazione e la diffusione dei dati sanitari che sono permesse solo con il consenso dell'interessato (art. 18 comma 1).

Vi sono tuttavia dei casi in cui la comunicazione o la diffusione dei dati sanitari sono ammesse anche in mancanza di consenso.

Innanzitutto la comunicazione è ammissibile quando è necessaria per il trattamento sanitario dell'interessato o dei suoi consanguinei o del convivente (art. 18 comma 1).

Inoltre la comunicazione può essere autorizzata dal Garante per esigenze di prevenzione o di cura, sia dei singoli che della collettività, sentito il parere del Consiglio Superiore di Sanità (art. 18 comma 2).

Infine la comunicazione o la diffusione dei dati sanitari sono ammesse, così come la diffusione degli altri dati personali, se fatte in forma anonima per scopi di studio o di ricerca (art. 19 lett. *a*)) ovvero per scopi concernenti la Sicurezza dello Stato e l'accertamento di reati (art. 19 lett. *b*)); la diffusione dei dati sanitari personali invece non è ammessa neppure nell'esercizio del diritto di cronaca (art. 18 comma 3).

8. La trasmissione dei dati personali oltre frontiera.

I dati elettronici possono essere diffusi non soltanto all'interno di un determinato Stato, ma anche all'estero. I modi con cui può avve-

nire la trasmissione dei dati oltre le frontiere di un determinato Paese sono diversi[42].

Il passaggio di frontiera dei dati, in particolare, può avvenire mediante un accesso diretto da parte di terminali o elaboratori situati all'estero a sistemi informativi situati in Italia; o da parte di terminali o elaboratori situati in Italia a sistemi informativi esteri; o all'interno di una organizzazione internazionale[43].

Il passaggio di frontiera dei dati dà luogo al sorgere di problemi, alcuni di natura giuridica, altri di natura più chiaramente politica.

I problemi giuridici nascono soprattutto dal fatto che la trasmissione dei dati oltre frontiera potrebbe comportare la violazione delle normative nazionali in tema di riservatezza. Alcuni dati personali, che non potrebbero essere diffusi in base alla normativa sulla riservatezza di un determinato Paese, potrebbero infatti circolare all'estero o addirittura essere ritrasmessi al Paese d'origine. Per ovviare a questi inconvenienti in molti ordinamenti sono stati inseriti, o si progetta di inserire, disposizioni in materia di trasmissione dei dati oltre frontiera.

In Italia il disegno di legge Martinazzoli prevedeva (cap. V) la trasmissione dei dati personali oltre frontiera dall'Italia all'estero (art. 20) e dall'estero in Italia (art. 21)[44].

Nel nuovo disegno di legge la disciplina della trasmissione dei dati personali oltre frontiera è, invece, contenuta nell'art. 20. Questo dispone: « Chiunque intenda trasferire fuori del territorio nazionale, con qualsiasi mezzo, dati personali assoggettati ad elaborazione informatica o raccolti allo scopo di assoggettarle a tale elaborazione, è tenuto a darne preventiva notificazione al Garante.

[42] I dati che riguardano l'Italia o i cittadini italiani, ad esempio, possono essere raccolti, memorizzati ed elaborati all'estero; oppure raccolti in Italia e memorizzati ed elaborati all'estero; o ancora raccolti, memorizzati ed elaborati in Italia e diffusi all'estero. Nel primo e nel secondo caso i dati passano la frontiera, in genere su supporti cartacei; nel terzo caso su supporti magnetici, e in particolare su nastri magnetici.

Può, naturalmente, verificarsi anche il caso contrario: dati riguardanti Paesi stranieri o cittadini stranieri possono essere raccolti, memorizzati ed elaborati all'estero; o ancora raccolti, memorizzati ed elaborati in Italia e diffusi all'estero. Nel primo e nel secondo caso i dati passano la frontiera, in genere su supporti cartacei; nel terzo caso su supporti magnetici, e in particolare su nastri magnetici.

[43] In questi casi i dati passano le frontiere attraverso le linee telefoniche normali o attraverso particolari reti internazionali di trasmissione dei dati tra le quali vanno citate Euronet-Diane, la Sita, la Nordic, la Datec e la Swift.

[44] Precisamente l'art. 20, intitolato modalità della trasmissione, disponeva:

« Chiunque intende trasferire fuori del territorio nazionale, con qualsiasi mezzo, dati personali assoggettati ad elaborazione informatica o raccolti allo scopo di assoggettarli a tale elaborazione, è tenuto a darne preventiva notificazione all'ufficio di controllo previsto dall'art. 5.

La notificazione deve contenere gli elementi di cui all'art. 4 ed è annotata in apposita sezione del registro generale previsto dall'art. 6 n. 5.

È vietato in ogni caso il trasferimento di dati personali in Paesi e tramite Paesi il cui ordinamento non preveda per essi una protezione almeno equivalente a quella prevista dalla presente legge ».

L'art. 21, invece, intitolato « Condizione di reciprocità » dispone: « Se la legge straniera prevede per la raccolta e la gestione di particolari categorie di dati personali norme di maggiore protezione rispetto a quelle previste dalla presente legge, si applicheranno le norme della legge straniera, sempreché l'ordinamento straniero preveda per i dati provenienti dal territorio italiano l'applicazione delle norme di maggiore protezione contenute nella presente legge ».

La notificazione deve contenere le indicazioni previste dall'art. 6 ed è annotata in apposita sezione del registro generale previsto dall'art. 10 n. 1.

Il trasferimento di dati personali fuori del territorio nazionale può essere vietato ove il Garante accerti che l'ordinamento del Paese al territorio del quale o tramite il territorio del quale ha luogo il trasferimento contiene norme in contrasto con la presente legge ».

I primi due commi corrispondono sostanzialmente ai primi due commi dell'analogo art. 20 del vecchio disegno di legge. Invece in parte difforme è il comma 3 e manca, inoltre, una norma analoga all'art. 21 del vecchio disegno di legge intitolato « Condizione di reciprocità ».

Una disciplina completamente diversa della trasmissione dei dati oltre frontiera è, invece, prevista nella proposta di direttiva della Commissione. Difatti a seguito della direttiva tutte le persone verranno a beneficiare in ogni Stato membro di una protezione dei dati personali equivalente e di elevato livello. Gli Stati membri, pertanto, non potranno più opporre alcuna restrizione alla circolazione di tali dati all'interno della Comunità.

La direttiva regola quindi la trasmissione dei dati personali non già all'interno della Comunità, ma esclusivamente nei Paesi terzi. Precisamente l'art. 24 afferma il principio secondo il quale il trasferimento di dati personali da uno Stato membro verso un Paese terzo può avere luogo soltanto a condizione che quest'ultimo garantisca un livello di protezione adeguato[45].

Peraltro in base al disposto dell'art. 25 uno Stato membro può derogare alle disposizioni dell'art. 24 paragrafo 1 per un determinato trasferimento di dati verso un paese terzo qualora il responsabile dimostri che nel caso di specie esistono sufficienti garanzie relativamente al rispetto di un livello di protezione adeguato[46].

[45] Art. 24. *Principi*. — 1. Gli Stati membri dispongono nella loro legislazione che il trasferimento temporaneo o definitivo, verso un paese terzo, di dati personali che formano oggetto di un trattamento, oppure raccolti a tal fine, può aver luogo soltanto a condizione che detto Paese garantisca un livello di protezione adeguato.

2. Gli Stati membri comunicano alla Commissione i casi in cui un paese terzo importatore non garantisce un livello di protezione adeguato.

3. Qualora la Commissione constati, in base alle informazioni degli Stati membri o in base ad altre informazioni, che un paese terzo non dispone di un livello di protezione adeguato e che la situazione che ne deriva è pregiudizievole per gli interessi della Comunità e dello Stato membro, essa può avviare negoziati al fine di porvi rimedio.

4. La Commissione può decidere, in conformità della procedura definita dall'art. 30, par. 2, che un paese terzo garantisce un livello di protezione adeguato in considerazione dei suoi impegni internazionali o della sua legislazione nazionale.

5. Le misure adottate a norma del presente articolo sono conformi agli obblighi incombenti alla Comunità in virtù di accordi internazionali, sia bilaterali che multilaterali, relativi alla protezione delle persone relativamente al trattamento automatizzato dei dati personali.

[46] Art. 25 § 1. Lo stesso articolo aggiunge che « lo Stato membro può accordare una deroga soltanto dopo averne informato la Commissione e gli Stati membri e se nessuno Stato membro o la Commissione notificano la loro opposizione entro un termine di dieci giorni. In caso di opposizione, la Commissione adotta le misure appropriate secondo la procedura di cui all'art. 30, par. 2.

È da tenere presente, altresì, la disposizione dell'art. 4 che fissa i criteri territoriali di applicazione della direttiva al fine di evitare sia i casi di elusione della legge sia i casi di cumulo di leggi. Il criterio adottato è quello del luogo in cui è situato l'archivio o risiede il responsabile.

La stessa norma precisa che se un archivio è suddiviso in vari sottoarchivi, localizzati in diversi Stati, ciascun sottoarchivio si considera un vero e proprio archivio a tutti gli effetti; e che, tuttavia, lo spostamento temporaneo di un archivio non costituisce un cambiamento di luogo.

La norma precisa ancora che l'utente che consulta un archivio situato in un Paese terzo mediante un terminale situato in uno Stato membro è tenuto a rispettare le disposizioni della direttiva; e che tale obbligo non sussiste in caso di utilizzazione sporadica.

È infine da tenere presente la Raccomandazione di decisione del Consiglio che prevede l'adesione delle stesse Comunità Europee alla Convenzione del Consiglio d'Europa sulla protezione delle persone nel trattamento automatizzato dei dati di carattere personale. Tale adesione garantirà la protezione delle persone interessate e la circolazione transfrontaliera dei dati personali nelle relazioni tra la Comunità e i paesi terzi aderenti; inoltre costituirà un incentivo per i Paesi terzi ad aderire alla Convenzione in modo da avere un libero scambio di dati con i Paesi della Comunità.

Una libera e corretta circolazione dei dati oltre frontiera presuppone peraltro una normativa internazionale uniforme.

Al riguardo la convenzione internazionale delle telecomunicazioni di Malaga-Torremolinos del 25 febbraio 1973 stabiliva il principio che il flusso internazionale dei dati anche personali avesse luogo senza ostacoli e interruzioni e in condizioni di segretezza fra i paesi firmatari.

L'art. 12 comma 2 della Convenzione del Consiglio d'Europa per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale dispone: « Una parte non può, al solo fine della protezione della vita privata, proibire o sottoporre ad una autorizzazione speciale i flussi attraverso i confini di dati a carattere personale destinati al territorio di un altro Stato ».

Peraltro il comma 3 aggiunge: « Tuttavia, ciascuna parte ha la facoltà di derogare alle disposizioni del comma 2:

a) nella misura in cui la sua legislazione preveda una regolamentazione specifica per certe categorie di dati a carattere personale o di schedari automatizzati di dati a carattere personale, a motivo della natura di tali dati o di tali schedari, salvo che la regolamentazione dell'altra Parte fornisca una protezione equivalente;

b) allorché il trasferimento è effettuato a partire dal suo territorio verso il territorio di uno Stato non contraente per il tramite del territorio di un'altra Parte, al fine di evitare che trasferimenti di questo tipo abbiano come risultato di aggirare la legislazione della Parte indicata all'inizio del presente comma ».

Gli aspetti politici sollevati dalla trasmissione dei dati oltre frontiera sono dati soprattutto dal fatto che le norme sulla protezione dei dati determinano all'interno un costo sociale e un sovracosto indotto da tali misure nelle imprese; e ciò può dar luogo ad uno squilibrio della competitività internazionale delle imprese. Inoltre i flussi non sono equilibrati: i paesi a tecnologia avanzata infatti sono in grado di raccogliere informazioni, accumularle e distribuirle coi sistemi informatici, mentre i paesi a civiltà tecnologica arretrata possono solo ricevere e consumare le informazioni.

Perfino negli scambi di informazioni tra USA e Europa vi è un forte divario. Si può in effetti ritenere che l'Europa fornisca agli Stati Uniti una larga porzione di dati bruti, senza valore aggiunto, mentre gli Stati Uniti forniscono all'Europa una grande quantità di dati elaborati e costosi.

In altri termini i flussi di informazione transatlantica corrispondono ad una esportazione di materia prima dei paesi tecnologicamente arretrati e ad una importazione di prodotto manufatturato; determina quindi ed accentua una condizione di sudditanza economica e scientifica.

La soluzione di tali problemi può derivare solo da un'efficace promozione dell'informatica in Europa e nei Paesi in via di sviluppo.

9. Le sanzioni penali.

Nei casi più gravi di inosservanza il disegno di legge prevede tre specie di reati: l'omessa o incompleta notificazione (art. 21), la comunicazione o la diffusione illecita (art. 22) e infine l'omessa custodia dei dati (art. 23).

Le norme ripetono le analoghe disposizioni contenute negli artt. 23, 27 e 26 del vecchio disegno di legge. Non sono state, invece, ripetute le norme relative all'inosservanza dei provvedimenti dell'ufficio di controllo (art. 24 vecchio disegno di legge), alla raccolta illecita (art. 25), alla omissione di cancellazione o di rettifica (art. 28), alla violazione del segreto di ufficio (art. 29), alle pene accessorie (art. 30) e alle disposizioni processuali (art. 31).

In tal modo il disegno di legge ha tenuto conto della nuova funzione del Garante rispetto a quella dell'Ufficio di controllo previsto dal disegno di legge Martinazzoli ed ha assunto nel suo complesso rispetto a quest'ultimo un carattere meno criminalizzante.

In effetti le disposizioni penali del primo disegno di legge avevano suscitato numerose critiche per la loro eccessiva severità: si era parlato a questo proposito di « terrorismo legislativo » e non era mancato chi aveva auspicato che il sistema sanzionatorio fosse limitato, al più, all'introduzione di sanzioni amministrative o pecuniarie.

Il secondo disegno di legge ha ritenuto invece « prive di efficacia, considerata la capacità finanziaria della grande maggioranza degli organismi che gestiscono le banche soggette a notificazione, sanzioni

di mero contenuto patrimoniale, soprattutto se di natura amministrativa »[47]; ha quindi mantenuto la previsione di specifiche figure di reato, pur limitandole alla violazione delle norme più significative; e ciò anche in conformità all'art. 23 della proposta di direttiva della Commissione[48].

[47] Relazione del gruppo di studio, p. 23. La Relazione riporta testualmente l'identico rilievo contenuto nella Relazione al d.d.l. Martinazzoli.

[48] Art. 23. (*Sanzioni*). — Gli Stati membri prevedono nelle loro legislazioni l'applicazione di sanzioni dissuasive al fine di garantire il rispetto delle disposizioni adottate in applicazione della presente direttiva ».