

ATTI PARLAMENTARI

XIII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. CXXXVI
n. 2

RELAZIONE

**SULL'ATTIVITÀ SVOLTA DAL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI
(ANNO 1998)**

(articolo 31, comma 1, lettera n), della legge 31 dicembre 1996, n. 675)

**Presentata dal Garante per la protezione dei dati personali
(RODOTÀ)**

Trasmessa alla Presidenza il 29 maggio 1999

PAGINA BIANCA

DISCORSO DEL PRESIDENTE STEFANO RODOTÀ	Pag.	IX
Elenco delle abbreviazioni		XXXV
Prefazione		XXXIX
1 L'EVOLUZIONE NORMATIVA NELL'ATTIVITÀ DEL PARLAMENTO E DEL GOVERNO		1
1.1 I provvedimenti normativi		1
1.2 L'attuazione della legge delega n. 676/1996		3
1.3 I provvedimenti normativi in campo internazionale		4
1.4 L'attività parlamentare in corso		5
2 TEMI DI MAGGIOR RILIEVO NELL'ATTIVITÀ DEL GARANTE		7
2.1 Pubbliche amministrazioni		7
2.1.1 Profili generali		7
2.1.2 Trasparenza dell'attività amministrativa		11
2.1.3 Diritto di accesso ai documenti amministrativi		15
2.1.4 Dati sensibili utilizzati dalla pubblica amministrazione		18
2.1.5 Documenti elettronici e carte magnetiche		20
2.1.6 Rete unitaria della pubblica amministrazione		21
2.1.7 Notificazione di atti giudiziari e amministrativi		23
2.1.8 «Riccometro» e «sanitometro»		25
2.1.9 Dichiarazioni dei redditi		28
2.1.10 Appalti		30
2.2 Informativa all'interessato e consenso		31
2.2.1 Complessità dei vecchi moduli e semplificazioni		31
2.2.2 Chiarezza delle informative ed esoneri		33
2.2.3 Libertà e specificità del consenso		34
2.3 Giornalismo e informazione		36
2.3.1 Lo sviluppo della l. n. 675/1996 in riferimento all'attività giornalistica		36
2.3.2 Il Codice deontologico		38
2.3.3 Prime applicazioni della nuova normativa		40
2.4 Associazioni e partiti politici		47
2.5 Confessioni religiose		49

2.6 Servizio sanitario nazionale	51
2.6.1 Profili generali	51
2.6.2 «Sanitometro»	55
2.6.3 Prescrizioni mediche	55
2.6.4 Tessera sanitaria	55
2.7 Previdenza e assistenza sociale	56
2.7.1 Previdenza ed enti previdenziali	56
2.8 Lavoro e legislazione sociale	57
2.9 Ricerca	58
2.9.1 Ricerca storica e archivi	58
2.9.2 Ricerca scientifica e statistica	63
2.9.3 Ricerca medica ed epidemiologica	64
2.10 Istituti di credito e assicurazioni	65
2.11 Intermediazione finanziaria	68
2.12 Informatica e telecomunicazioni	69
2.12.1 Telefonia e servizi di telecomunicazioni	69
2.12.1.1 La nuova normativa di tutela nelle telecomunicazioni	69
2.12.1.2 Prime esperienze applicative	71
2.12.2 Video-sorveglianza	73
2.12.3 Commercio elettronico	77
2.13 Flussi transfrontalieri di dati	80
2.13.1 Profili generali	80
2.13.1.1 Alcuni casi applicativi	81
2.13.2 Trasferimento di dati verso gli USA	82
2.14 Trattamento di dati per finalità di giustizia	82
2.15 Servizi di sicurezza e attività di polizia	85
2.15.1 Trattamenti effettuati dal Ced del Dipartimento della pubblica sicurezza e dalle forze di polizia	85
2.15.2 Archivi NSIS, Schengen e SIRENE	86
2.15.3 Servizi di sicurezza	86

3 IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI	87

3.1 Competenze e attività	87
3.1.1 Ricorsi	87
3.1.2 Segnalazioni e reclami	90
3.1.3 Attività consultive	90
3.1.3.1 La consultazione dal parte del Parlamento	90
3.1.3.2 La consultazione dal parte del Governo	91
3.1.4 Autorizzazioni al trattamento dei dati sensibili	95
3.1.4.1 Le autorizzazioni generali	95
3.1.4.2 Le autorizzazioni <i>ad hoc</i>	97

3.1.5 Rapporti con l'Ufficio del Garante	98
3.1.6 Registro generale dei trattamenti	99
3.1.6.1 Il quadro normativo	99
3.1.6.2 L'organizzazione	100
3.1.6.3 Prospettive	101
3.1.7 Attività ispettiva	103
3.2 L'Ufficio del Garante	105
3.2.1 Regolamento sull'organizzazione e il funzionamento dell'Ufficio	105
3.2.2 Il decreto legislativo concernente l'Ufficio	106
3.2.3 La gestione delle risorse umane	108
3.2.4 Codice etico	110
3.2.5 Attività seminariali	111
3.2.6 Relazioni esterne, rapporti con i media	111
3.2.7 La gestione finanziaria	113
3.2.8 Informatizzazione	115
3.2.9 Creazione di un Centro di documentazione	117
3.2.10 Assetto organizzativo per il 1998	118
3.2.11 Sede dell'Ufficio	120
3.2.12 Dati sulle principali attività del Garante	121
3.2.13 Indagine conoscitiva	122
4 ATTIVITÀ COMUNITARIE E INTERNAZIONALI	123
4.1 Premessa	123
4.2 Normativa comunitaria	124
4.2.1 La direttiva-quadro n. 95/46/CE e la direttiva n. 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni	124
4.2.2 Quadro comparativo sul recepimento delle direttive 95/46/CE e 97/66/CE nei Paesi membri dell'Ue	125
4.2.3 Lo sviluppo della Società dell'Informazione e l'attività della Commissione europea: le proposte di direttiva relative a un quadro comune sulle firme elettroniche e all'armonizzazione di alcuni aspetti del commercio elettronico	129
4.3 La cooperazione europea nei settori giustizia e affari interni	131
4.3.1 Consiglio giustizia e affari interni (Trattato di Amsterdam e proposta italiana per una omogeneizzazione)	131
4.3.2 Schengen	131
4.3.3 Europol	132
4.3.4 Sistema informativo doganale	133
4.3.5 Eurodac	134
4.4 Consiglio d'Europa	134
4.5 Organizzazione per la cooperazione e lo sviluppo (OCSE)	135
4.6 Collaborazione con Autorità di garanzia di altri Paesi	135
4.7 Partecipazione a convegni e incontri internazionali	136

5 ALLEGATI	137
5.1 Legge n. 675 del 31 dicembre 1996	137
5.2 Legge n. 676 del 31 dicembre 1996	166
5.3 d.P.R. n. 501 del 31 marzo 1998 – Regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'art. 33, comma 3, della legge 31 dicembre 1996, n. 675	169
5.4 Codice etico del Garante per la protezione dei dati personali	190
5.5 Provvedimento 29 luglio 1998 - Codice di deontologia giornalistica	194
5.6 Autorizzazioni generali al trattamento di dati sensibili	199
5.6.1 Autorizzazione n. 1/98 - Rapporti di lavoro	199
5.6.2 Autorizzazione n. 2/98 - Stato di salute e vita sessuale	204
5.6.3 Autorizzazione n. 3/98 - Organismi di tipo associativo	211
5.6.4 Autorizzazione n. 4/98 - Liberi professionisti	216
5.6.5 Autorizzazione n. 5/98 - Diverse categorie di titolari	221
5.6.6 Autorizzazione n. 6/98 - Investigatori privati	229
5.7 Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali	234
5.7.1 Documento di lavoro: notifica	234
5.7.2 Utilizzazione di disposizioni contrattuali nel trasferimento di dati personali verso Paesi terzi	241
5.7.3 Raccomandazione 1/98 in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo	252
5.7.4 Parere 1/98 - Preferenze in materia di protezione della vita privata e la «norma aperta per i profili»	256
5.7.5 Trasferimento di dati personali verso Paesi terzi	259
5.7.6 Documenti di lavoro sulla procedura relativa alla valutazione dei codici di condotta comunitari	291
5.7.7 Parere 1/99 - Il livello di protezione dei dati negli Stati Uniti e il dibattito in corso	294
5.8 Commissione europea	297
5.8.1 Progetto di direttiva per le firme elettroniche	297
5.8.2 Proposta di direttiva sul commercio elettronico	311
5.9 Autorità di controllo comune Schengen	315
5.9.1 2ª Relazione di attività (marzo 1997 - marzo 1998)	315
5.9.2 Parere n. 98/1 - Conservazione dei dossier	331
5.9.3 Parere n. 98/2 - Segnalazione di persone la cui identità è stata usurpata	333

5.9.4	Parere n. 98/3 - Relazioni tra il Sistema d'informazione Schengen e il progetto «ASF - veicoli rubati»	335
5.9.5	Parere n. 98/4 - Registrazione delle consultazioni di cui all'art. 103 della Convenzione	338
5.9.6	Relazione sulla sicurezza degli uffici SIRENE	340
5.9.7	Dichiarazione in occasione del 50° Anniversario della dichiarazione universale dei diritti dell'uomo	342
5.10	Consiglio d'Europa	343
5.10.1	Raccomandazione 99 (5) - Linee guida per la <i>privacy</i> su Internet	343
5.10.2	Schema di raccomandazione - Protezione dei dati personali raccolti e trattati per scopi assicurativi	349
5.10.3	Decisione del Consiglio dell'Unione Europea con cui si autorizza la Commissione a negoziare emendamenti alla Convenzione n. 108	358
5.10.4	Schema degli emendamenti alla Convenzione 108 (T-PD (98) 31)	360
5.10.5	Documento di lavoro 31/98: schema di protocollo aggiuntivo alla Convenzione 108	364
5.11	Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	367
5.11.1	Conferenza ministeriale di Ottawa: 7-9 ottobre 1998	367

PAGINA BIANCA



Garante

per la protezione dei dati personali

RELAZIONE PER L'ANNO 1998

**DISCORSO DEL PRESIDENTE
STEFANO RODOTÀ**

Roma, 12 aprile 1999

PAGINA BIANCA

Signor Presidente della Repubblica,

come definire, a due anni dall'inizio della sua attività, il Garante per la protezione dei dati personali? Una "istituzione di frontiera", forse, anche se si tratta di una espressione tutt'altro che originale. Ma è proprio lì, su una frontiera, che il Garante lavora, misurandosi ogni giorno con problemi inediti e ostinate resistenze, muovendosi tra incomprensioni e incitamenti e, come accade a chiunque stia su una frontiera incerta e contestata, gli è capitato anche di trovarsi tra due fuochi.

Una frontiera istituzionale, economica, sociale, culturale. Non si comprenderebbe la singolare vicenda che si è aperta ai primi di maggio del 1997 se non si tenessero nel giusto conto tutte queste dimensioni. Infatti, la legge sulla tutela dei dati personali si è via via rivelata come un dato forte, persino ingombrante, che obbligava a mettere in discussione certezze consolidate, abitudini amministrative e scientifiche, e a dare una diversa ricostruzione del sistema nel suo complesso.

Tutto questo ha determinato pure spaesamenti e ansie, che il Garante si è impegnato a fugare con un lavoro collegiale di adattamento dei principi alle molteplici situazioni considerate dalla legge. Alle certezze promosse dal Garante, tuttavia, si chiede di far seguire quelle che possono venire da norme più analitiche: e ciò avverrà,

grazie ai decreti delegati che prevedono specifiche discipline in determinati settori. Ma bisogna guardarsi anche dal rischio di irrigidire il sistema con troppe regole di dettaglio, che lo priverebbero della flessibilità indispensabile in una materia in costante divenire, dominata dall'incessante mutamento determinato dalle innovazioni scientifiche e tecnologiche.

Si è misurata, intanto, una influenza che non rimaneva nel chiuso cerchio delle norme giuridiche. Lo dico con uno spirito che è, insieme, di orgoglio e timore: non v'è alcun paese al mondo dove una legge come questa abbia suscitato risposte così intense dei cittadini, reazioni delle istituzioni e del sistema delle imprese, attenzioni continue e persino aggressive del sistema della comunicazione. La conferma è nelle cifre. Tra il marzo del 1998 e quello del 1999 i maggiori giornali nazionali hanno dedicato ai problemi della privacy 2500 pagine, di cui 600 alla specifica attività del Garante. Ventisettemila richieste dei cittadini nel primo anno di attività potevano far pensare (e forse sperare, visto lo scarto tra l'immane lavoro e le ridotte dimensioni dell'ufficio) che si trattasse soltanto di una fiammata iniziale, dovuta alla novità, ed agli interrogativi che questa provocava. Così non è stato. Il nostro secondo anno è stato accompagnato da ventimila richieste, sì che a questo punto s'impone una riflessione sulle ragioni del permanere di una attenzione tanto forte. Una analisi qualitativa deve seguire la rilevazione quantitativa.

E' legittimo un dubbio. E se tutta questa attenzione fosse dovuta soprattutto alle difficoltà determinate dalla legge, che spingono ad interrogare continuamente il Garante? Una analisi dell'insieme dei

ricorsi, reclami, segnalazioni e quesiti ci dice che non è così. Esistono richieste in cui si esprimono difficoltà oggettive e soggettive: ma si tratta di una percentuale ridotta, che si può stimare intorno al dieci per cento del totale, sicuramente fisiologica, e che scompare del tutto se si esaminano le richieste avanzate in forma di ricorso.

La grandissima parte delle richieste, quindi, ha radici e motivazioni ben diverse, che possono essere raggruppate in tre filoni. Si può parlare di una "privacy/rispetto", invocata da tutti quelli che, finalmente, dispongono di strumenti efficaci per respingere indebite invasioni e discriminazioni, e così sviluppare pienamente la loro personalità; di una "privacy/alibi", dietro la quale si trincerano quanti vogliono sottrarsi al controllo o coprire inefficienze; di un intreccio tra "privacy e trasparenza", che si è manifestato nei moltissimi interventi del Garante volti ad eliminare barriere alla conoscenza di dati significativi, che non trovavano alcun fondamento nella legge. Vi è, poi, un numero ridotto di richieste che esprimono esigenze che non possono essere soddisfatte attraverso gli strumenti previsti per la tutela dei dati personali, e che tuttavia meritano d'essere considerate perché in esse, probabilmente, è una delle chiavi interpretative per comprendere la spinta dei cittadini verso il Garante.

Qui si manifesta non tanto un travisamento dei fini della legge, quanto piuttosto un estremo tentativo di arrivare alla soluzione di problemi incancreniti. Il Garante per la protezione dei dati personali si presenta così come una istituzione "scialuppa", dove si cerca di salire quando ogni altro appiglio sembra perduto, come una sorta di difensore civico senza confini. E' ovvio che, in casi come questi, il

Garante comunica di non poter intervenire. Ma l'atteggiamento di chi considera il Garante come l'unico appiglio si ritrova anche in casi in cui è certa la sua competenza. E allora bisogna dire con franchezza che il flusso delle richieste esprime anche una sorta di distacco da altre istituzioni, ed un trasferimento delle attese verso una istituzione appena creata, quasi che questa potesse ricostituire un circuito di fiducia che altrove appare spezzato.

In questo atteggiamento si può certo cogliere il rischio d'una distorsione. In realtà, siamo di fronte ad un effetto della innovazione più significativa introdotta dalla legge n. 675: il trasferimento al cittadino del diritto di governare direttamente i propri dati personali ha determinato una redistribuzione di poteri che non poteva non investire nel suo insieme il sistema istituzionale.

Proprio partendo da questa constatazione, abbiamo fatto la scelta - impegnativa, ma a nostro giudizio obbligata - di cercar di rendere al massimo agevole l'accesso al Garante, di spogiarlo d'ogni formalismo e, di conseguenza, di rispondere a tutte le richieste. Ho parlato di scelta obbligata, perchè la novità del sistema non consiste nell'aver creato un organo al quale il cittadino deve necessariamente rivolgersi quando viene messo in discussione o violato uno dei suoi nuovi diritti. L'innovazione vera sta nell'aver costituito ogni cittadino come garante di se stesso, dal momento che ciascuno può direttamente curare la tutela dei propri diritti senza alcuna intermediazione burocratica. Anzi, i ricorsi al Garante, previsti dall'art. 29 della legge, sono in via generale ammissibili solo dopo che i diritti indicati dall'art. 13 siano stati esercitati nei confronti del responsabile.

S'impone, a questo punto, un'altra considerazione. La dimensione quantitativa dell'"utenza" della legge n. 675 non può essere misurata solo con il riferimento, già imponente, alle quarantasettemila richieste al Garante. In questa cifra, infatti, non è compreso il numero di cittadini che si sono rivolti direttamente alle amministrazioni pubbliche o al settore privato per far valere i diritti riconosciuti dalla legge n. 675. Molteplici indizi, tratti da diversi materiali di cui disponiamo, ci dicono che si tratta di un fenomeno ormai diffuso: ma non siamo in grado di misurarne l'ampiezza e la frequenza. Un dato, tuttavia, merita d'essere riferito. In diversi settori, molti hanno avvertito come un fastidio l'invio di moduli d'informativa e di richieste di consenso al trattamento dei dati, lamentando soprattutto la loro prolissità e oscurità (di questo ci siamo preoccupati, e proprio in questi giorni abbiamo messo a punto un nuovo schema, estremamente semplificato). Molti altri, però, hanno percepito che in quel fastidio era contenuta pure una opportunità: più di tre milioni e mezzo di clienti delle banche hanno chiesto di ricevere solo i materiali strettamente necessari per la gestione del loro rapporto con la banca. Un "sondaggio di massa", se così vogliamo chiamarlo, davvero senza precedenti, e che merita d'essere attentamente considerato per comprendere le diverse valenze sociali ed economiche della disciplina dei dati personali, se a queste si guarda partendo dal suo primo protagonista, il cittadino.

Ma v'è un'altra considerazione che impone di guardare ai quarantasettemila casi come ad un punto di partenza e non come ad un dato definitivo. Vi sono provvedimenti del Garante che, pur riferiti ad un soggetto specifico, in realtà riguardano una pluralità di soggetti, fino ad interessare la totalità dei cittadini. E' quel che è accaduto, ad

esempio, quando si sono affrontate questioni riguardanti la salute, le notificazioni giudiziarie, il traffico telefonico. E non si tratta di effetti indiretti: in questi casi, il provvedimento del Garante modifica immediatamente la condizione di tutti i potenziali interessati. Siamo di fronte ad una tutela con effetti collettivi.

Questo, dunque, è il circuito istituzionale e sociale che si va delineando, con innovazioni notevoli e problemi di cui non può essere sottovalutata la portata. In questo circuito si manifesta la presenza anche di soggetti che possono arricchirne il significato e rendere più agevole la trasmissione delle domande sociali. E' già avvenuto che taluni temi siano stati segnalati al Garante da difensori civici locali, che finiscono così con l'adempire ad una duplice funzione: rilevazione di questioni significative e selezione di quelle più rilevanti. L'importanza della dimensione locale, peraltro, è stata ben considerata dal Garante che ha sottoscritto con l'Anci una convenzione per la diffusione dei suoi provvedimenti riguardanti l'amministrazione locale, e per "formare i formatori" in un settore nuovo e complesso. Si intravedono così occasioni di decentramento che possono consentire una migliore percezione ed utilizzazione della disciplina di tutela dei dati personali.

Accanto all'articolazione territoriale si colloca quella sociale, di cui può essere buona espressione l'iniziativa delle associazioni dei consumatori, che ha avuto un ruolo significativo nell'avvio dell'attività del Garante, la cui prima pronuncia rispondeva appunto a loro sollecitazioni. Ora è possibile che la nuova disciplina delle associazioni

rappresentative dei consumatori determini una loro maggior presenza nel complesso circuito istituzionale individuato dalla legge n. 675.

Parlare di un nuovo circuito istituzionale, che sta prendendo forma, non è una forzatura, determinata da una pretesa di attribuire al Garante una posizione di particolare rilievo. Il tipo di richieste rivolte al Garante, i soggetti che le alimentano, le risposte del Garante e i loro effetti collettivi mostrano che siamo di fronte non solo ad una istituzione di garanzia, ma ad un insieme di strumenti e di procedure che possono contribuire ad una più diffusa e radicata democrazia dei cittadini.

Non sono parole. La nostra Relazione è, in primo luogo, un catalogo dei casi in cui sono cresciuti i diritti di tutti, non di un manipolo di privilegiati. E' la testimonianza di come sia possibile eliminare discriminazioni odiose dei più deboli, ammalati di Aids o portatori di handicap. E' l'indicazione concreta del modo in cui si possono respingere piccole e grandi prevaricazioni di amministrazioni pubbliche o di poteri privati, si tratti dei questionari sottoposti a dipendenti comunali o dei test sul posto di lavoro, dei rapporti con l'amministrazione fiscale o dell'uso dei dati nelle indagini giudiziarie. Gli ammalati guadagnano rispetto, ai consumatori viene data voce. Emergono i diritti dei cittadini nel sistema delle telecomunicazioni, nei rapporti con i gestori dei diversi servizi. Si affrontano le questioni di un futuro già presente - il controllo capillare dei cittadini attraverso reti internazionali, schedature, videosorveglianza

Nella discussione pubblica, così intensa da risultare persino sorprendente, questa dimensione è talvolta oscurata da una accezione

ristretta e inadeguata del termine "privacy", ormai entrato stabilmente nel linguaggio comune. Si è detto che la propensione dei cittadini non è tanto quella di cercare maggiore riservatezza, quanto l'opposto desiderio di apparire, di esibirsi, di denudarsi in pubblico. Si è aggiunto che troppo diverso è l'humus culturale di un paese come l'Italia perché possa attecchire una pianta nata e cresciuta nel ben diverso ambiente degli Stati Uniti. Si è sottolineato il rischio di un crescente isolamento individuale, di un allentarsi dei legami sociali, che proprio l'accento posto sulla privacy potrebbe determinare.

E' questa la frontiera culturale dalla quale il Garante non può ritrarsi, proprio perché la legge stessa gli dà il compito di contribuire a definire davanti all'opinione pubblica il significato della tutela dei dati personali. E allora bisogna ricordare che la società dell'informazione e della comunicazione non genera spinte tutte convergenti. Convivono al suo interno pulsioni diverse, tutte parimenti forti: il bisogno di notorietà, per il quale nessun prezzo è troppo alto, fosse pure il sacrificio d'ogni pudore o intimità; e la richiesta imperiosa di rispetto o di silenzio, estesa anzi anche ad aree che in passato non l'avevano conosciuta. Sono, se si vuole, culture a confronto. E chi crede che la cultura del rispetto, di sé in primo luogo, meriti d'essere secondata, ha oggi a disposizione uno strumento che prima mancava.

Peraltro, negli stessi Stati Uniti dall'antico bozzolo del "diritto ad essere lasciato solo" è progressivamente uscita una nozione più ricca e comprensiva di privacy, che ne fa una condizione della cittadinanza, una premessa per un comprensivo statuto delle informazioni persona-

li, uno strumento per la definizione di relazioni personali e sociali, dunque di quella "vita comune" che per l'individuo è condizione di esistenza. Trasferita in Europa, questa nozione non solo non ha trovato difficoltà ad attecchire ma, incontrandosi con la tradizione della tutela legislativa dei diritti dell'uomo, si è irrobustita al punto da raggiungere un livello di tutela che oggi non ha pari nel mondo. Ed è proprio qui, in questo paradossale divario tra una tutela che s'indebolisce nel paese d'origine e si rafforza nel continente europeo, che s'innesta la dialettica tra Unione Europea e Stati Uniti per quanto riguarda il trasferimento in quest'ultimo paese dei dati personali trattati in Europa, perché si dubita che il sistema statunitense offra quell'"adequata protezione" che la Direttiva 95/46 esige nel paese di destinazione, per evitare la creazione di "paradisi dei dati" che vanificherebbero la tutela raggiunta dai cittadini europei.

In questo confronto il Garante italiano ha avuto un ruolo di rilievo, tanto che sotto la sua presidenza è stato possibile giungere ad un documento unanime dei garanti europei sulla trattativa ancora in corso. Si dilata così la dimensione istituzionale, che condiziona anche i diritti dei cittadini italiani e, quindi, impone al Garante un continuo allargamento dei confini della sua azione, con una crescita degli stessi impegni quotidiani che è stato possibile fronteggiare solo grazie al permanere nell'intero personale di una tensione e di una abnegazione particolari.

Infatti, mentre il Garante si trovava a partecipare come protagonista alla nascita di un nuovo circuito istituzionale, si palesavano difficoltà non trascurabili all'interno dei circuiti formali e consolidati.

Lunga è stata l'attesa del regolamento, pubblicato sulla Gazzetta ufficiale solo il 1 febbraio 1999 (d.P.R. 31 marzo 1998, n. 501); faticoso è stato l'approdo, sempre nel febbraio di quest'anno, ad un provvedimento indispensabile, quello che definisce la complessiva situazione del personale (d.l. 26 febbraio 1999, n. 51); difficile permane il rapporto con alcune strutture amministrative.

Dobbiamo dar atto alla Presidenza del Consiglio dello sforzo fatto nell'ultima fase per chiudere definitivamente la partita organizzativa, sì che oggi possiamo ben dire che i maggiori problemi sono alle nostre spalle, anche se non sarà breve il tempo necessario per tradurre i provvedimenti in concrete attività organizzative. Permangono, invece, diversi altri problemi, in primo luogo quelli legati alla mancata consultazione del Garante, come vuole l'art. 31.2 della legge n. 675, su diversi atti normativi e amministrativi che pure interessavano la protezione dei dati personali e contenevano specifiche norme in materia. Qui non sono tanto le prerogative formali del Garante ad essere vulnerate: sono messe in discussione le garanzie dei cittadini per la cui salvaguardia, appunto, si è voluto prevedere il parere obbligatorio del Garante. Peraltro, la mancanza di tale parere determina un vizio della procedura di adozione dei provvedimenti con immaginabili e non lievi conseguenze. Ci auguriamo, quindi, che una più energica azione della Presidenza del Consiglio possa consentire il definitivo superamento di questa situazione, che certamente non favorisce il buon andamento dell'azione amministrativa.

Di alcuni atteggiamenti dell'amministrazione, ad ogni modo, conviene parlare ancora per un momento. La documentazione delle

resistenze al cambiamento da parte di ogni apparato appartiene da tempo agli studi sulle organizzazioni pubbliche e private. Ma è nostro preciso dovere ricordare che in molti casi, puntualmente documentati nella Relazione, queste resistenze hanno provocato carenze nell'informazione dei cittadini, mancata nomina di responsabili e incaricati dei trattamenti, genericità della regolamentazione di cornice di nuovi strumenti rilevanti per il trattamento di dati personali, ritardo nell'emanazione di atti importanti anche per il settore privato, come il regolamento di sicurezza. Ma, soprattutto, qui si è talvolta manifestato un ritorno verso una chiusura della macchina amministrativa, che ha fatto ricorso alla "privacy-alibi" per cercar di ridurre la trasparenza dell'attività, costringendo il Garante ad interventi che lo hanno trasformato, come si è detto, in un vero e proprio Garante "della trasparenza". L'amministrazione rischia così di contribuire al diffondersi e al radicarsi di un fenomeno che ci preoccupa assai, e al quale ci ripromettiamo di dedicare la massima attenzione nei prossimi mesi, cioè una disapplicazione della legge anche in momenti e situazioni di particolare rilevanza.

Al Garante potrebbe esser mosso un rimprovero, appunto quello di non aver esercitato in questa direzione un'adeguata vigilanza, anche perché, proprio in occasione della presentazione della Relazione dell'anno scorso, si era manifestata la consapevolezza del problema. Bisogna, tuttavia, tener conto di due fattori. Il primo riguardava l'assenza del regolamento, e dunque di tutte le garanzie legate allo svolgimento di una attività ispettiva che può avere conseguenze assai pesanti, anche sul piano penale, una volta accertate violazioni della legge. Il secondo era legato all'esiguità del personale, che

ha imposto un ordine di priorità nel quale risultavano assolutamente preminenti i provvedimenti relativi al fiume di segnalazioni, reclami, quesiti, ricorsi.

Ora quest'insieme di fattori negativi è, almeno formalmente, superato. Ci avviamo, quindi, verso una fase nella quale l'attività di ispezione andrà via via assumendo la sua giusta importanza, né vesatoria, né compiacente. Un'attività indispensabile: non solo per cancellare sacche di non applicazione della legge, ma anche per evitare disparità di trattamento, soprattutto nel settore privato, tra operatori che hanno attuato la disciplina sui dati personali, sopportando i relativi costi, e operatori che disapplicano la legge, raccolgono i dati in maniera scorretta e finiscono così con l'esercitare anche una forma di concorrenza sleale, che danneggia altri imprenditori e vanifica le garanzie per i cittadini. Queste non sono soltanto ipotesi. Informazioni da noi raccolte sull'andamento in alcuni settori, come quello del direct marketing, provano come l'attenta applicazione della legge n. 675 abbia avuto anche effetti di moralizzazione, eliminando operatori poco corretti o scarsamente affidabili.

E' evidente che questi comportamenti virtuosi potranno proseguire e radicarsi, determinando quel mutamento culturale che poi è la ragione stessa della legge, solo se il Garante sarà capace di dare una continua e piena assicurazione di efficienza. E questa, per gli organismi che si pongono come interlocutori diretti dei cittadini, viene di solito misurata attraverso la capacità di risposta istituzionale, e le attese più o meno lunghe dei cittadini.

L'analisi dei dati relativi a questo aspetto dell'attività del Garante richiede alcune distinzioni. Se si volesse semplificare, e dare una interpretazione blandamente trionfalistica del nostro lavoro, si potrebbe mettere l'accento sul fatto che, per quanto riguarda lo strumento più importante nelle mani dei cittadini, cioè i ricorsi, non esiste nessun arretrato. Si può aggiungere, anzi, che la decisione del Garante arriva in tempi brevissimi, i venti giorni prescritti dalla legge, anche se proprio l'esperienza di queste ultime settimane ci fa ritenere che un termine più congruo potrebbe consentire una più adeguata presenza delle parti ed un miglior approfondimento delle questioni, come vuole la natura di "giustizia alternativa" che caratterizza questo aspetto dell'attività del Garante.

Ma non ci si può fermare a questo dato, pur relevantissimo, senza velare la realtà complessiva e rischiare di cadere prigionieri d'una contraddizione. Si ricordava prima che una delle decisioni più impegnative del Garante è stata quella di offrire ai cittadini un accesso ampio e non formalizzato: non si può trascurare, quindi, la situazione relativa a segnalazioni, reclami, quesiti, che rappresentano la gran massa delle richieste rivolte al Garante. Qui l'esiguità delle risorse a disposizione dell'ufficio ha determinato ritardi, che non possono essere sottovalutati. E' vero che molte richieste hanno ricevuto indiretta risposta attraverso provvedimenti del Garante che decidevano questioni analoghe o prossime; attraverso l'opera di chiarimento, anche telefonico, della portata della legge; attraverso pareri generali dati ad organismi rappresentativi di intere categorie. E tuttavia queste considerazioni ci sembrano insufficienti, sì che abbiamo già deciso di destinare al presidio di questa frontiera forze ben più consistenti di

quelle finora disponibili, e che non era possibile accrescere fino a che non fossero state approvate le norme sull'aumento del personale.

E' per questo motivo, e non per una modesta mania di grandezza, che abbiamo insistito presso Governo e Parlamento perché al Garante fossero messi a disposizione i mezzi umani e finanziari indispensabili per svolgere un compito la cui ampiezza non era prevedibile al momento dell'entrata in vigore della legge. Muovendosi in tale direzione, non è necessario considerare soltanto la dimensione quantitativa. Davanti a noi sta pure il compito di definire più precisi e rigorosi percorsi procedurali anche per gli strumenti diversi dai ricorsi, ai quali si affida la grande maggioranza dei cittadini. Queste sono regole che il Garante può definire autonomamente, grazie ai poteri che ormai gli sono stati riconosciuti.

Sia per disegnare meglio le modalità del proprio agire, sia per stimolare la necessaria cooperazione di altre istituzioni, dunque, rimane indispensabile una continua iniziativa del Garante. Che, tuttavia, non può essere autoreferenziale, finalizzata unicamente alla maggiore efficienza dell'ufficio. E' la stessa legge ad imporgli il dovere di segnalare al Governo l'opportunità di provvedimenti legislativi richiesti dall'evoluzione del settore e di stimolare una produzione normativa qualitativamente diversa, che coinvolga le categorie interessate, approdando a codici di deontologia e buona condotta, che il Garante verifica e di cui contribuisce a garantire diffusione e rispetto.

Il nuovo circuito istituzionale si arricchisce così in una ulteriore direzione, con una significativa innovazione sul terreno delle fonti

del diritto. E' una dinamica che si coglie già nella dimensione internazionale e che, accanto ai tradizionali "produttori" di norme, vede crescere il ruolo di altri soggetti, in particolare privati. A questi si riconoscono spazi di autonomia, che tuttavia non si presentano come fine a se stessi, ma rappresentano la premessa di forme originali di integrazione con l'azione di soggetti pubblici.

In Italia questa tendenza ha avuto la manifestazione più significativa nel Codice di deontologia dell'attività giornalistica, entrato in vigore il 29 luglio 1998. L'innovazione è grande perché, dietro la formula tradizionale del codice deontologico, in realtà si trova una normativa secondaria che, pur fondata sulla previsione dell'art. 25 della legge n. 675, è il risultato della collaborazione tra il Consiglio nazionale dell'Ordine dei giornalisti e il Garante per la protezione dei dati personali. Si tratta di un insieme di norme che si rivolgono a tutti coloro i quali operano nel sistema dell'informazione, iscritti o no all'albo dei giornalisti; sono applicabili quindi anche in sede giurisdizionale; e, soprattutto, trovano la loro fonte immediata in un potere affidato integralmente ad un soggetto privato (l'Ordine) e ad una autorità indipendente.

Il Codice è nato tra furibonde polemiche, suscitate soprattutto da chi indicava in quel testo uno strumento limitativo del diritto d'informazione e nel Garante l'incarnazione di un nuovo censore. Ora quelle polemiche, più che infondate, appaiono lontane, e al suo posto troviamo significativi riconoscimenti di tutte le associazioni rappresentative dei giornalisti, che hanno indicato quel testo come un significati-

vo punto di equilibrio tra due valori in eterna tensione, cronaca e riservatezza. E, con il passare del tempo, è probabile che si apprezzerà sempre di più che le regole contenute in quel codice rappresentano pure un importante elemento di garanzia per i giornalisti, la cui attività non potrà essere più giudicata secondo criteri, non dirò arbitrari, ma eccessivamente discrezionali.

Questa vicenda, ad ogni modo, ha proiettato il Garante sulla frontiera certamente più esposta, quella appunto del sistema dell'informazione, essenziale per la comunicazione tra il Garante e i cittadini, ma che può anche determinare una presentazione della nostra attività comprensibilmente condizionata dalle specifiche esigenze professionali dei giornalisti. E tuttavia, malgrado distorsioni e incomprensioni, molti timori e molti fantasmi sono stati dissipati dalla forza dei fatti, dall'esperienza concreta di questi pochi mesi.

Quando, ad esempio, il Garante intervenne nella materia dei cosiddetti "fuori onda", segnalando la necessità di evitare la diffusione di immagini raccolte all'insaputa di un soggetto invitato ad una trasmissione per finalità diverse, non ci si limitò ad esercitare un più che legittimo diritto di critica verso quella decisione. Con toni aggressivi si disse che non sarebbe stato più possibile render note indiscrezioni, diffondere foto che non fossero "posate", e via dicendo.

Nessuna di queste previsioni pessimistiche si è verificata. E non perché il Garante abbia poi adottato interpretazioni più "benevole",

ma perché nulla nel suo provvedimento autorizzava quella conclusione. Questo non vuol dire che siano mancate difficoltà, tuttavia legate spesso al fatto che l'entrata in vigore della legge n. 675 ha, in questa materia come altrove, amplificato segnali in passato deboli, determinato una rinnovata attenzione istituzionale e sociale per norme a tutela della riservatezza che, già presenti nell'ordinamento, erano tuttavia inapplicate. Si coglie qui un altro effetto di sistema di questa legge, consistente appunto nell'aver dato un centro ed una rinnovata forza a discipline sparse e disorganiche (norme sui minori, sulla violenza sessuale, sull'uso delle manette), con una particolare evidenza della "privacy-rispetto".

Al di là delle singole vicende, nel sistema dell'informazione è venuta crescendo una spontanea adesione non tanto a questa o quella norma della legge n. 675, quanto piuttosto ai valori che questa intende promuovere. Non è un caso che il Codice di deontologia, e significative decisioni del Garante, facciano intenso riferimento alla dignità della persona come costante ed ineliminabile principio di riferimento.

Il segno della percezione dell'alto significato di questa prospettiva si coglie non soltanto nella più rispettosa presentazione di molte notizie, ma negli interventi di molti ordini regionali e, soprattutto, nel fatto che a sollecitare l'intervento del Garante siano stati, in casi particolarmente delicati, gli stessi giornalisti, individualmente o attraverso i loro organismi associativi. Tuttavia, proprio l'analisi di questi casi, come quello triste e recente della ragazza uccisa a

Gravina, ha messo in evidenza come all'origine di molte notizie giudicate lesive della riservatezza vi sia non un comportamento aggressivo del giornalista, ma la violazione di segreti investigativi, professionali, d'ufficio. Il Garante ha così evitato di indicare nei giornalisti gli unici responsabili di eventuali violazioni, e ha preso specifiche iniziative per impedire "alla fonte" il sorgere di tali violazioni. In questa prospettiva si è rivelata particolarmente importante la collaborazione con la Polizia di Stato, l'Arma dei Carabinieri, la Guardia di Finanza e la Polizia penitenziaria, che stanno mettendo a punto regole per evitare, fuori dei casi in cui ciò corrisponde a necessità istituzionali, le traduzioni in manette e la diffusione di foto segnaletiche.

Ma non corrisponderebbe alla realtà dei fatti una rappresentazione dei rapporti tra sistema dell'informazione e attività del Garante integralmente risolta nella crescita di limitazioni. Il Garante ha agito e continua ad agire come "istituzione della trasparenza", tanto che quasi un terzo dei suoi provvedimenti va proprio in questa direzione. E' così cresciuta la disponibilità di informazioni rilevanti alle quali i giornalisti possono liberamente accedere, come dimostrano diversi provvedimenti, relativi ad esempio a retribuzioni e incarichi. Lungi dall'essere compresso, il giornalismo d'inchiesta trova così nuovi canali e materiali.

La costruzione progressiva di un nuovo circuito istituzionale, tuttavia, non può passare soltanto attraverso comportamenti virtuosi e interpretazioni che valorizzano la nuova dimensione individuata

dalla legge n. 675 e dai suoi principi. E' indispensabile il completamento del sistema voluto dal legislatore attraverso la delega contenuta nella legge n. 676 e il suo rinnovo. Alcuni decreti legislativi sono già stati emanati, ma rimangono da regolare materie complesse e di grandissima rilevanza, come sono quelle che riguardano i dati sensibili di cui dispone la pubblica amministrazione, i dati sulla salute, l'attività di direct marketing, le reti telematiche, e quindi uno dei fenomeni oggi più importanti su scala mondiale, Internet. I futuri decreti delegati, inoltre, offriranno pure l'occasione per risolvere alcuni problemi applicativi sottolineati dall'esperienza di questi due anni, che il Garante ha già messo in evidenza e ora segnala nella sua Relazione.

E' probabile che, una volta completato l'intervento legislativo, divenga necessaria la redazione di un vero e proprio testo unico, che non solo renda immediatamente percepibile l'ampiezza del nuovo quadro normativo, ma ne faciliti la comprensione. Continuiamo a rilevare, infatti, casi di scarsa attenzione per la stessa lettera delle norme. Questa constatazione sollecita il Garante a promuovere una conoscenza più diretta e un accesso più immediato all'insieme delle norme, ai suoi provvedimenti e a tutto il materiale rilevante, compreso quello internazionale. L'ormai imminente apertura del nostro sito Web e di un centro di documentazione, la previsione di borse di ricerca contribuiranno alla creazione di una indispensabile cultura diffusa.

Questo è tanto più necessario in quanto la tutela dei dati personali non costituisce una materia compatta, in qualche modo settoriale. Si diffonde, invece, in tutta la società, in ogni sua articolazione,

investe l'attività economica, i comportamenti istituzionali, le scelte individuali. E' quindi più difficile, o comunque più lenta, la nascita di "esperti della privacy", capaci di abbracciare ogni interesse e ogni settore. Viene così confermata la necessità di una forte presenza del Garante, tuttavia né accentratrice né autoritaria, ma che mantenga e promuova significative forme di collaborazione nei diversi settori, come peraltro già avviene.

Mi limito qui a ricordare che, confermando una prassi seguita nel passato, il Garante ha promosso consultazioni informali attraverso la pubblicazione di bozze di suoi documenti sulla stampa, sollecitando le osservazioni di tutti gli interessati. Ha svolto indagini conoscitive, come quella che ha riguardato gli oltre 800 modelli sottoposti ai clienti delle diverse banche o quella, appena avviata, sulla videosorveglianza, che è fenomeno che si diffonde con straordinaria rapidità, sul quale il Garante è già intervenuto e che, comunque, richiede un tempestivo intervento legislativo.

Torna così il tema dell'infinita frontiera lungo la quale si distende l'attività del Garante. Che diventa ancor più impegnativa se si considera la dimensione internazionale, anzi mondiale, dei problemi, com'è nella natura stessa della società dell'informazione. Qui, nel flusso incessante di dati che percorre il mondo, i confini nazionali sono una convenzione sempre più precaria, e quindi la stessa tutela delle informazioni personali esige regole comuni e forme di coordinamento che diano vita ad un circuito istituzionale che superi le frontiere.

Tra mille difficoltà e resistenze, soprattutto da parte di chi pensa che le regole del mercato possano sostituire ogni altra regola, la costruzione di questo circuito va avanti. E qui il ruolo dell'Italia è quello di un paese che conosce molte precarietà tecnologiche, ma che sul piano istituzionale è riuscito a guadagnare una posizione di primissimo piano, sopravanzando anche paesi di più lunga tradizione. Si sommano la tempestiva trasposizione delle direttive europee sui dati personali e sui servizi di telecomunicazioni, le norme sul documento elettronico e la firma digitale, le iniziative per l'informatica nella pubblica amministrazione, le sperimentazioni delle reti civiche, la costituzione di un comitato dei ministri e di un forum per la società dell'informazione. Si delineano i tratti di una organizzazione istituzionale e sociale pronta a frequentare il futuro. Ma, proprio per questo, è necessaria un'azione più convinta, che componga in un disegno coerente e incisivo le diverse iniziative, e che non perda mai di vista l'esigenza di tutelare i diritti e le libertà fondamentali, come esplicitamente vuole l'art. 1 della legge n. 675.

La Relazione, che oggi presentiamo, vuol essere un contributo anche in questa direzione, nel suo sforzo non solo di rendere conto di una attività, ma pure di delineare i tragitti istituzionali che determina. Ripetiamo l'auspicio, che già formulavamo l'anno passato, di una sua discussione in Parlamento.

Questa può rappresentare uno dei momenti più significativi per meglio definire il ruolo delle autorità indipendenti, come auspicava il Presidente della Repubblica intervenendo proprio alla presentazione della nostra Relazione dell'anno scorso. Conosciamo le polemiche che,

nella fase più recente, hanno riguardato queste istituzioni. E penso che siamo tutti consapevoli della necessità di non mettere a rischio proprio quell'indipendenza che è la loro ragion d'essere.

Ma un ripensamento è necessario, anche per chiarire, come già aveva cercato di fare la Commissione bicamerale per le riforme istituzionali, quali siano i requisiti perché si possa dire d'essere davvero in presenza d'una autorità indipendente. D'altra parte, già si delineano i diversi strumenti che consentono di mantenere piena l'indipendenza, senza però trasformarla in separazione istituzionale: discussione parlamentare delle relazioni, audizioni da parte delle Camere, confronti a livello europeo, procedure di massima trasparenza, controllo giurisdizionale sui provvedimenti, controllo contabile sull'attività.

Ma ogni meccanismo istituzionale non deve perdere di vista i valori da tutelare. Il Garante ha respinto la tentazione, sempre presente purtroppo in una parte della cultura giuridica, di considerare le indicazioni di principio contenute nell'art. 1 della legge come una pura enunciazione retorica, priva di concreta portata normativa. I riferimenti ai diritti ed alle libertà fondamentali, al principio della dignità della persona, sono stati la sua bussola.

E' per questa ineludibile ragione che in diversi settori, da quello fiscale a quello delle indagini di polizia, abbiamo incessantemente richiamato l'attenzione sulla necessità di non abbandonarsi ad una deriva tecnologica che, utilizzando le infinite e crescenti possibilità di trattamento delle informazioni, avvolga la società intera in una rete a

maglie fittissime. Proprio perché vogliamo che si possa continuare a parlare di “tecnologie della libertà”, dobbiamo evitare che lo strumento tecnologico venga invece piegato alla costruzione di una società della sorveglianza e della classificazione. Dobbiamo evitare un inquinamento tecnologico dell’ambiente delle libertà civili e politiche. Riteniamo che il Parlamento abbia voluto il Garante come presidio dei nuovi diritti nella società dell’informazione.

Nell’azione nostra quotidiana pensiamo d’aver contribuito all’inveramento di essenziali valori costituzionali. Anche in questo secondo anno di attività crediamo d’aver operato per liberare la tutela dei dati personali dall’angustia delle interpretazioni che vorrebbero chiuderla in una sorta di presidio dell’egoismo. Abbiamo cercato, in ogni momento, di guardare ad essa come ad una componente essenziale della cittadinanza, dunque come ad uno strumento per un complessivo arricchimento individuale e sociale.

Il lavoro era, e rimane, difficile. Thomas Stearns Eliot diceva che non possiamo “sopportare troppa realtà”. Ma proprio al carico del reale non è dato sottrarci. E non per presunzione, ma perché questo è il compito che ci è stato affidato.

PAGINA BIANCA

La presente relazione è riferita al 1998 e contiene alcune notizie ulteriori, aggiornate al 19 marzo 1999, relative a taluni sviluppi significativi che si è ritenuto opportuno menzionare.

ELENCO DELLE ABBREVIAZIONI

<i>art.</i>	articolo
<i>c.c.</i>	codice civile
<i>c.p.c.</i>	codice di procedura civile
<i>c.p.p.</i>	codice di procedura penale
<i>cd.</i>	cosiddetto/a
<i>cfr.</i>	confronta
<i>Cost.</i>	Costituzione
<i>d.l.</i>	decreto legge
<i>d.lg.</i>	decreto legislativo
<i>d.m.</i>	decreto ministeriale
<i>d.P.C.M.</i>	decreto del Presidente del Consiglio dei ministri
<i>d.P.R.</i>	decreto del Presidente della Repubblica
<i>G.U.</i>	Gazzetta Ufficiale
<i>l.</i>	legge
<i>lett.</i>	lettera
<i>n.</i>	numero
<i>p.</i>	pagina
<i>Pa</i>	pubblica amministrazione
<i>pag.</i>	pagina
<i>provv.</i>	provvedimento
<i>r.d.</i>	regio decreto
<i>reg.</i>	regolamento
<i>s.r.l.</i>	società a responsabilità limitata
<i>T.U.</i>	testo unico
<i>u.s.</i>	ultimo scorso
<i>Ue</i>	Unione europea
<i>v.</i>	vedi

Bollettino «Cittadini e Società dell'Informazione», Bollettino del Garante per la protezione dei dati personali.

PAGINA BIANCA

Garante per la protezione dei dati personali

Presidente

Stefano RODOTÀ

Componenti

Giuseppe SANTANIELLO, *Vice Presidente*

Ugo DE SIERVO

Claudio MANGANELLI

Segretario generale

Giovanni BUTTARELLI

PAGINA BIANCA

PREFAZIONE

Questa seconda relazione coglie il Garante per la protezione dei dati personali in un momento di passaggio difficile da un avvio avventuroso ad una stabilità ancora non raggiunta. Si sono via via delineati, con chiarezza crescente, i suoi rapporti con l'amministrazione pubblica e con il multiforme settore privato. Si è consolidato, soprattutto, il suo rapporto con i cittadini lungo una frontiera lunga e mobile, che non ignora quasi nessun problema della vita individuale e sociale. È divenuto sempre più evidente che l'innovazione introdotta dalla legge 31 dicembre 1996, n. 675, ha creato un circuito istituzionale nuovo, nel quale interviene una molteplicità di soggetti e che prospetta sfaccettature molteplici dei rapporti tra pubblico e privato, tra opacità e trasparenza. La dimensione internazionale fa sentire il suo peso, e si distende sulle aree dove maggiore e più immediata è l'influenza delle nuove tecnologie.

Nel corso del secondo anno di attività si è manifestato con forza lo scarto tra ampiezza dei compiti e risorse limitate. Per questo è stato importante che, proprio verso la sua conclusione, siano arrivati provvedimenti importanti per la definitiva organizzazione del Garante, il regolamento e il decreto legislativo riguardante il personale e le risorse finanziarie. Da qui può ora cominciare uno sforzo che metta l'ufficio in condizione di fronteggiare in modo adeguato l'insieme delle richieste che gli vengono rivolte, e di estendere la sua attività ad aree che, come quella delle ispezioni, sono state finora trascurate.

Non è possibile apprezzare i diversi aspetti dell'attività del Garante fuori d'una cronaca minuta e puntuale di tutte le sue iniziative. La relazione ne dà una presentazione organizzata e sistematica. Viene così fornita una informazione che può consentire a tutti gli interessati di orientarsi meglio in una materia che quasi non conosce confini. Al tempo stesso, si propone una riflessione complessiva su una attività multiforme, che può consentirne una migliore valutazione, anche critica.

PAGINA BIANCA

1 L'EVOLUZIONE NORMATIVA NELL'ATTIVITÀ DEL PARLAMENTO E DEL GOVERNO

1.1 I PROVVEDIMENTI NORMATIVI

Nel corso dell'anno sono stati adottati dal Parlamento, dal Governo o da singoli Ministri numerosi provvedimenti normativi (atti aventi forza di legge, regolamenti governativi o ministeriali) che incidono più o meno direttamente sui diritti della personalità (in particolare sulla riservatezza, la dignità umana e l'identità personale), oltre ad alcuni decreti legislativi che hanno dato attuazione alla l. 31 dicembre 1996, n. 676 («Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»).

In alcuni casi, a riprova di una maggiore consapevolezza dell'importanza della materia avvertita dagli organi istituzionali, sono state proposte o adottate disposizioni già in origine conformi alla normativa introdotta dalla l. 31 dicembre 1996, n. 675 («Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»).

In altri casi, invece, il Garante ha formulato suggerimenti e rilievi, sottolineando l'opportunità di integrare o modificare alcuni provvedimenti *in itinere* in considerazione dei riflessi che le scelte avrebbero altrimenti comportato sui diritti della persona e sulla stessa l. n. 675/1996.

Pertanto, questa Autorità ha dovuto purtroppo constatare che alcuni regolamenti governativi e ministeriali sono stati adottati senza la previa consultazione del Garante, benché l'art. 31, comma 2, della l. n. 675/1996 preveda espressamente tale consultazione da parte del Presidente del Consiglio dei ministri e di ciascun ministro all'atto della predisposizione di norme regolamentari suscettibili di incidere sulle materie disciplinate dalla legge. Di tutti questi casi si tratterà diffusamente più avanti, unitamente ai regolamenti e ai provvedimenti amministrativi generali sui quali il Garante è stato ritualmente consultato (v. § 3.1.3.2).

Vari provvedimenti normativi saranno descritti più in dettaglio nel testo della relazione, nell'ambito delle materie cui si riferiscono. È opportuno però fornire un quadro riassuntivo dei provvedimenti più importanti, sui quali l'Autorità ha formulato suggerimenti o che comunque incidono, con norme espresse, sulle materie di sua competenza:

- il Garante ha fornito spunti di riflessione nell'*iter* di approvazione della l. 16 giugno 1998, n. 191 (cd. «Bassanini-ter») circa la necessità di rendere meglio compatibili con la l. n. 675/1996 e con i principi contenuti nella legge delega n. 676/1996 alcune disposizioni riguardanti il rilascio della carta d'identità con strumenti informatici, le modalità di sottoscrizione delle istanze rivolte alla pubblica amministrazione, il codice fiscale e il «telelavoro» nella pubblica amministrazione. In proposito, nel corso della seduta della Camera del 27 maggio 1998, il Governo ha accolto un ordine del giorno presentato da alcuni parlamentari (Jervolino Russo, Cerulli Irelli, Di Bisceglie, Corsini) con il quale si è impegnato ad attuare le richiamate disposizioni in armonia con i decreti legislativi che saranno adottati in base alla l. n. 676/1996 (ora anche in base alla l. 6 ottobre 1998, n. 344);

- sono stati seguiti attentamente i lavori parlamentari di conversione del d.l. 21 settembre 1998, n. 328, in ordine a una disposizione sul trattamento dei dati delle persone da reclutare per la nomina a giudice onorario delle sezioni-stralcio destinate

al recupero dell'arretrato nel processo civile (art. 1, comma 9, l. 19 novembre 1998, n. 399). Alla Camera, benché preannunciato dal relatore della competente commissione, non è stato presentato un emendamento tendente ad adeguare la disposizione descritta ai principi della l. n. 675/1996, emendamento che era stato auspicato dal Garante. Tuttavia, il 17 novembre 1998 il Governo ha accolto un ordine del giorno presentato dall'on. Senese durante i lavori della Commissione giustizia del Senato con il quale, preso atto che la norma introdotta non è pienamente conforme ai predetti principi, in particolare per quanto attiene alle garanzie previste per i trattamenti dei dati «sensibili» effettuati da soggetti pubblici, il Governo si è impegnato a reconsiderarne i contenuti in occasione dell'emanazione del decreto legislativo organico su tale ultima materia che dovrà essere adottato entro l'8 maggio 1999 (v. cap. 1.2 e § 2.1.4);

– durante i lavori di discussione del disegno di legge «collegato» alla finanziaria 1999 (poi approvato con l. 23 dicembre 1998, n. 448), questa Autorità ha segnalato, su richiesta della Commissione bilancio della Camera (che era stata sensibilizzata al riguardo dalla Presidenza della Camera su impulso di alcuni gruppi parlamentari), l'esigenza di adeguare ai principi della l. n. 675/1996 una norma concernente il collegamento telematico fra le banche dati dell'amministrazione finanziaria e quelle di altri soggetti, pubblici o privati, a fini di accertamento fiscale. La norma è stata quindi stralciata dal testo originario per essere approfondita e resa conforme ai richiamati principi della l. n. 675/1996 per quanto riguarda, in particolare, le modalità di raccolta e di utilizzazione di alcuni dati «sensibili» (AC 5267-ter «Disposizioni in materia di collegamento dell'Amministrazione finanziaria con altre banche dati»). La medesima disposizione, tuttavia, è stata successivamente presentata in forma di emendamento governativo al disegno di legge recante «Disposizioni in materia di perequazione, razionalizzazione e federalismo fiscale» (AC 3599) in discussione presso la Commissione finanze e tesoro del Senato. La discussione ha permesso però di approfondire il tema e di migliorare la formulazione della norma approvata dall'Aula unitamente al d.d.l., il 18 marzo 1999;

– in occasione della conversione del cd. «decreto Di Bella» in materia di sperimentazioni cliniche in campo oncologico e altre misure in materia sanitaria (d.l. 17 febbraio 1998, n. 23), il Garante aveva sottoposto alla Commissione igiene e sanità del Senato alcune osservazioni in materia di compilazione e conservazione delle ricette mediche, nonché in tema di consenso informato, che sono state recepite attraverso appositi emendamenti. I suggerimenti hanno trovato accoglimento anche nel testo della legge di conversione (l. 8 aprile 1998, n. 94, v. § 2.1.4);

– il Garante ha, inoltre, constatato con soddisfazione che il Parlamento ha ritenuto opportuno far acquisire il parere di questa Autorità in ordine agli schemi dei decreti legislativi previsti dalla l. n. 449/1997 («collegato» alla finanziaria 1998), in tema di fissazione dei criteri di valutazione della situazione economica dei cittadini ai fini della erogazione di determinate prestazioni sociali (cd. «riccometro») o dell'esenzione dal costo di prestazioni sanitarie (cd. «sanitometro»). Il Garante, constatato che in diversi punti i due provvedimenti incidevano sulla riservatezza dei dati personali, ha quindi formulato due articolati pareri con i quali ha invitato il Governo a perfezionarne gli schemi in linea con i richiamati principi della l. n. 675/1996 (v. § 2.1.8).

Quanto ai provvedimenti normativi che incidono più direttamente sui diritti della personalità e sulla riservatezza dei dati personali, e per i quali il Garante non è stato coinvolto o che comunque non denotano profili critici, si segnalano:

– la l. 28 settembre 1998, n. 337, recante delega al Governo per il riordino della disciplina in materia di riscossione, che reca una norma in base alla quale la revisione delle disposizioni in materia di notifica degli atti esattoriali dovrà essere effettuata tenuto conto della normativa sulla tutela dei dati personali (art. 1, comma 1, lett. i)). Alcune parti della delega sono state attuate con il d.lg. 22 febbraio 1999, n. 37, che disciplina i versamenti mediante delega ai concessionari rinviando a una convenzione da approvarsi con decreto ministeriale (art. 1, comma 2); altre trovano considerazione nell'art. 12 del d.lg. 26 febbraio 1999, n. 46, in tema di notificazione della cartella di pagamento, che prevede però la notifica in plico chiuso solo in caso di invio di raccomandata con avviso di ricevimento e non anche per la notifica in altre forme. Il Garante è stato da ultimo invitato l'8 marzo 1999 dal Ministro delle finanze a collaborare alla definizione di un d.m. che, in relazione a quanto previsto dalla l. n. 337/1998 e dai successivi decreti delegati, dovrà disciplinare l'accesso telematico dei concessionari ai dati dei debitori iscritti a ruolo dei coobbligati;

– il d.lg. 5 giugno 1998, n. 204, in materia di ricerca scientifica e università, il quale contiene una norma elaborata con la collaborazione del Garante, la quale, in linea con quanto previsto dall'art. 27 della l. n. 675/1996, consente alle pubbliche amministrazioni, e in particolare alle università, la diffusione di dati relativi a determinate categorie di soggetti (laureati, ricercatori, ecc.) al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico. Ciò nel rispetto delle garanzie previste dalla medesima l. n. 675/1996 (art. 6, comma 4);

– il d.P.R. 24 giugno 1998, n. 249, recante lo statuto degli studenti della scuola secondaria, che riconosce il diritto dello studente alla riservatezza (art. 2, comma 2). È questo uno dei primi casi in cui il diritto alla riservatezza, garantito in via generale dalla l. n. 675/1996, viene espressamente richiamato in una specifica normativa di settore.

1.2 L'ATTUAZIONE DELLA LEGGE DELEGA N. 676/1996

Per quanto riguarda l'attuazione della legge delega n. 676/1996, sono stati seguiti con particolare attenzione i lavori preparatori della l. 6 ottobre 1998, n. 344, che ne ha prorogato il termine di scadenza fino al 31 luglio 1999, introducendo peraltro un opportuno vaglio preventivo delle competenti commissioni parlamentari sugli schemi dei decreti legislativi. Il Governo e il Parlamento hanno ritenuto necessaria la proroga per l'obiettivo complessità degli interventi richiesti soprattutto in alcuni settori (dati sanitari, dati utilizzati a fini storici o di ricerca, *direct marketing*, servizi di informazione e comunicazione per via telematica, trattamenti parzialmente «esclusi» dall'ambito di applicazione della l. n. 675/1996, ecc.).

Il Garante è stato consultato poi sugli schemi dei decreti legislativi con i quali il Governo ha prorogato sino all'8 maggio 1999 il regime transitorio dei trattamenti dei dati sensibili effettuati dai soggetti pubblici, previsto dall'art. 41, comma 5, della l. n. 675/1996 (decreti legislativi 8 maggio 1998, n. 135 e 6 novembre 1998, n. 389). Entro quella data il Governo dovrà adottare la disciplina «a regime» di tale importante profilo. Al riguardo giova rilevare che in occasione del rilascio del parere sulla conformità alla delega del d.lg. n. 389/1998, la Commissione giustizia del Senato, il 4 novembre 1998, ha sottolineato l'opportunità che il Governo provveda in materia con un unico, organico, provvedimento normativo che contenga disposizioni pienamente rispettose dello spirito e della lettera della l. n. 675/1996.

In proposito va anche ricordato che il Garante aveva partecipato in precedenza alla messa a punto di un primo schema di decreto legislativo sul trattamento dei dati sensibili nella pubblica amministrazione, approvato dal Consiglio dei ministri il 22 luglio 1998, ma che non risulta emanato.

Nell'occasione, questa Autorità ha segnalato l'insufficienza del complessivo livello di protezione dei dati ipotizzato dal provvedimento, rispetto alle garanzie previste dall'art. 22, comma 3, della l. n. 675/1996, in particolare per quanto attiene ai contenuti delle leggi di «copertura» dei trattamenti pubblici e all'ipotizzata, mera, «comunicazione» al Garante dei trattamenti effettuati, però, senza una precisa normativa di garanzia. Nella medesima circostanza, il Garante ha però constatato che il testo diramato presentava alcune disposizioni che avrebbero opportunamente incrementato il grado di tutela delle persone (obbligo per i soggetti pubblici di adottare misure che facilitino l'esercizio dei diritti di cui all'art. 13 della l. n. 675/1996; principio di «essenzialità» dei dati trattati; obbligo di verifiche periodiche sulla correttezza e legittimità dei dati alla stregua dell'art. 9 della citata legge; adozione di tecniche di cifratura dei dati o di sistemi di conservazione separata degli stessi a fini di sicurezza).

Un'ulteriore consultazione del Garante si è poi avuta con riguardo allo schema del d.lg. 13 maggio 1998, n. 171, meglio esaminato nel prosieguo, con il quale sono state dettate norme di tutela della vita privata nel settore delle telecomunicazioni, anche in attuazione della direttiva 97/66/CE, nonché disposizioni in tema di attività giornalistica (v. § 2.12.1 e 2.3.1).

Sotto quest'ultimo aspetto occorre altresì ricordare che, in linea con il compito attribuitogli dalla l. n. 675/1996 di promuovere presso le categorie interessate la sottoscrizione di codici di deontologia, il Garante, con un provvedimento del 29 luglio 1998 (pubblicato sulla G.U. n. 179 del 3 agosto 1998), ha portato a un utile e soddisfacente esito la cooperazione con il Consiglio nazionale dell'Ordine dei giornalisti volta all'approvazione del nuovo codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, di cui ha disposto la pubblicazione nella «Gazzetta Ufficiale».

1.3 I PROVVEDIMENTI NORMATIVI IN CAMPO INTERNAZIONALE

Il Garante ha seguito i lavori parlamentari relativi all'approvazione dei disegni di legge di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia-Europol (l. 23 marzo 1998, n. 93), nonché della convenzione sull'uso dell'informatica nel settore doganale con il connesso protocollo sull'interpretazione in via pregiudiziale da parte della Corte di giustizia (ll. 30 luglio 1998, n. 291 e 292).

Tali convenzioni contengono importanti disposizioni sulla protezione dei dati personali trattati nei rispettivi sistemi informativi (archivi Europol e SID), finalizzate alla prevenzione e repressione di determinati reati o infrazioni amministrative nel campo della criminalità organizzata e nel settore doganale.

Di particolare interesse per l'attività del Garante è risultata inoltre la l. 5 febbraio 1999, n. 25 («legge comunitaria per il 1998»), che menziona, fra gli atti comunitari cui dare completa attuazione, la direttiva comunitaria n. 95/46/CE in materia di protezione di dati personali.

Quanto, infine, ai provvedimenti all'esame del Parlamento, il Garante continuerà a seguire i lavori concernenti il disegno di legge di ratifica ed esecuzione del protocollo sui privilegi e sulle immunità del personale di Europol (AC 4954) e lo schema di decreto legislativo di attuazione della direttiva 96/9/CE sulla tutela giuridica delle banche dati, approvato in via preliminare dal Consiglio dei ministri il 3 dicembre 1998.

1.4 L'ATTIVITÀ PARLAMENTARE IN CORSO

Nell'ambito dei prossimi impegni, il Garante proseguirà l'esame dei lavori parlamentari di alcuni provvedimenti normativi che recano disposizioni attinenti alla protezione dei dati personali. Si segnalano, in particolare:

- il disegno di legge in materia di diritto d'asilo (AC 5381);
- i provvedimenti attinenti alle intercettazioni telefoniche (testo unificato dell'AC 2773 del Governo e proposte abbinate), ai servizi di telefonia (AC 2519) e alle notifiche di atti giudiziari (AS 3699 del Governo e proposte abbinate);
- il testo unificato in materia di telelavoro (AA.SS. 2305, 3123, 3189, 3489);
- il disegno di legge che ridisciplina la trasmissione dei dati contenuti nelle cd. «schede d'albergo» (testo unificato dell'AC 5003 e proposte abbinate);
- i provvedimenti riguardanti l'attività regolamentare delle Autorità indipendenti (AACC 1665, 4868 e 5151) e le incompatibilità dei loro componenti (AS 3236 del Governo);
- i provvedimenti attinenti a notificazioni di atti giudiziari (AA.SS. 2751, 2974, 3615, 3639, 3699).

PAGINA BIANCA

2. TEMI DI MAGGIOR RILIEVO NELL'ATTIVITÀ DEL GARANTE

2.1 PUBBLICHE AMMINISTRAZIONI

2.1.1 Profili generali

La l. n. 675/1996, come è noto, regola anche i trattamenti di dati personali effettuati dalle amministrazioni pubbliche, prevedendo nei loro confronti una disciplina parzialmente diversa da quella applicabile ai privati e agli enti pubblici economici.

Il Garante, nel corso del 1998, è stato chiamato più volte a chiarire come opera tale disciplina e a precisare che i soggetti pubblici non devono richiedere il consenso agli interessati, dovendo piuttosto verificare che i trattamenti effettuati rispettino i presupposti e i limiti previsti.

La disciplina in esame mantiene, peraltro, la distinzione fra i trattamenti di dati cd. «particolari» (quelli previsti dagli artt. 22 e 24 della legge) e i trattamenti relativi ad altri dati. Infatti, come è noto:

- a) i soggetti pubblici possono trattare dati personali «comuni» soltanto per lo svolgimento delle funzioni istituzionali e nei limiti stabiliti dalle leggi e dai regolamenti vigenti nei settori di riferimento (art. 27, comma 1).

Nell'ambito delle varie operazioni di trattamento la fase che merita più attenzione è spesso rappresentata dalla eventuale comunicazione o diffusione dei dati trattati; la legge ha perciò stabilito che debbano essere rispettati alcuni specifici presupposti, che sono diversificati a seconda che la divulgazione di dati avvenga verso un altro soggetto pubblico o nei confronti di soggetti privati.

Nel primo caso è necessario che la comunicazione o la diffusione siano previste da una norma di legge o di regolamento oppure, in via strettamente residuale, che esse siano necessarie per lo svolgimento delle funzioni istituzionali; in quest'ultima ipotesi occorre darne preventiva comunicazione al Garante, che può eventualmente vietarle (art. 27, comma 2).

A questo proposito si deve rilevare che sono pervenute a questa Autorità numerose comunicazioni ai sensi dell'art. 27, comma 2, alcune delle quali, tuttavia, si sono rivelate scarsamente utili perché segnalavano flussi di dati tra Pa già disciplinati da norme di legge o di regolamento. Viceversa, in riferimento ai casi in cui tali flussi non sono ancora espressamente regolamentati, non si è avuta notizia di una diffusa attivazione da parte delle Pa per l'adozione di normative specifiche che tengano conto dei principi stabiliti dalla l. n. 675/1996 in materia di comunicazione di dati personali tra soggetti pubblici.

Si deve tuttavia riconoscere che in alcuni casi l'impulso di questa Autorità ha trovato un riscontro effettivo: si veda ad esempio l'art. 21 della l. 24 giugno 1997, n. 196 («Norme in materia di promozione dell'occupazione») che, alla luce dei suggerimenti forniti dal Garante nel giugno 1997 (v. *Relazione per l'anno 1997*, pag. 83), ha integrato la normativa in materia di liste di mobilità dei lavoratori prevedendo espressamente l'obbligo per le imprese, oltre che per l'INPS, di comunicare i nominativi dei lavoratori alla Commissione regionale per l'impiego.

Ancora, il Ministero dell'università e della ricerca scientifica, tenendo conto delle indicazioni di questa Autorità, ha provveduto a modificare il testo del d.m. 23 aprile 1998 in materia di trattamento dei dati relativi alle preiscrizioni universitarie.

Se invece la comunicazione o la diffusione di dati personali avviene da un soggetto pubblico verso un soggetto privato o verso un ente pubblico economico, non è possibile - neanche in via residuale - operare in base a un mero riferimento alle finalità istituzionali, in quanto occorre comunque una specifica norma di legge o di regolamento che preveda la divulgazione.

Si rileva al riguardo che la mancanza di siffatte disposizioni legislative o regolamentari ha costretto alcune amministrazioni a interrompere diversi flussi di comunicazioni di dati verso soggetti privati o enti pubblici economici. Si ricorda in particolare il parere espresso dal Garante il 19 dicembre 1998 in ordine alla possibilità, per un istituto tecnico industriale statale, di trasmettere a una società privata l'elenco degli studenti diplomati negli ultimi due anni, completo delle informazioni relative a data di nascita, indirizzo, recapito telefonico, voto conseguito e anno di diploma.

In tale provvedimento il Garante, dopo aver osservato che dall'esame delle disposizioni vigenti in materia di istruzione secondaria superiore (in particolare, d.lg. 16 aprile 1994, n. 297; l. 10 dicembre 1997, n. 425 e d.P.R. 23 luglio 1998, n. 323) non emergono norme che consentono di trasmettere a privati elenchi o altre raccolte di dati relativi ai diplomati, ha invitato il competente Ministero a promuovere l'adozione di un'apposita disposizione, anche regolamentare, che disciplini i presupposti, le finalità e le garanzie dell'eventuale rilascio nei confronti di aziende e di altri soggetti di elenchi di diplomati, anche per scopi diversi da quelli di assunzione, ma egualmente meritevoli di considerazione;

- b) quando i dati sono invece di carattere «particolare» la disciplina richiede maggiori garanzie. I soggetti pubblici, per poter effettuare una o più operazioni di trattamento - comprese la comunicazione e la diffusione - sui dati «sensibili» (che l'art. 22, comma 1 individua tra quelli idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a partiti politici, sindacati, associazioni, lo stato di salute e le abitudini sessuali), hanno infatti bisogno di essere «autorizzati» da una espressa e dettagliata disposizione di legge che preveda quali dati possono essere trattati, le operazioni che possono essere eseguite su di essi e le rilevanti finalità di interesse pubblico perseguite (art. 22, comma 3).

Lo stesso requisito è richiesto affinché i predetti soggetti possano trattare i dati idonei a rivelare l'esistenza di alcuni provvedimenti giudiziari, indicati all'art. 24 della legge. In tale caso, tuttavia, in assenza di una specifica norma di legge, l'autorizzazione può essere fornita con provvedimento del Garante.

Il quadro normativo si sarebbe dovuto completare rapidamente. L'art. 41, comma 5 della l. n. 675/1996 aveva previsto originariamente che i trattamenti dei dati «particolari» da parte dei soggetti pubblici, iniziati prima dell'entrata in vigore della legge, potessero essere proseguiti - anche in assenza delle espresse disposizioni di legge sopra indicate - fino all'8 maggio 1998. È stata invece disposta una proroga di tale termine dapprima fino all'8 novembre 1998 (d.lg. n. 135/1998) e, da ultimo, fino all'8 maggio 1999 (d.lg. n. 389/1998).

Resta comunque fermo il profilo relativo al consenso. L'Autorità ha infatti precisato più volte che il consenso, se per i soggetti pubblici - come si è detto - non è necessario, tanto meno può essere richiesto agli interessati per legittimare un trattamento che non rispetti i requisiti previsti dagli artt. 22, 24 o 27 (ad esempio, attraverso il consenso dell'interessato non è possibile comunicare dati personali a soggetti privati se ciò non è previsto da una norma di legge o di regolamento).

L'unica eccezione a tale meccanismo è quella prevista in materia di dati sanitari (art. 23). Infatti, come si vedrà (§ 2.6.1), gli organismi sanitari pubblici possono trattare i dati idonei a rivelare le condizioni di salute dell'interessato facendo riferimento a una specifica norma di legge che li autorizzi secondo quanto previsto dall'art. 22, comma 3, oppure (utilizzando l'altra soluzione prevista dall'art. 23, comma 1) avvalendosi del consenso dell'interessato o dell'autorizzazione del Garante, a seconda delle finalità perseguite.

La particolare normativa stabilita per i soggetti pubblici, specie in riferimento alla comunicazione e alla diffusione dei dati, ha creato qualche problema di corretta interpretazione da parte dei medesimi soggetti, testimoniata dai diversi quesiti pervenuti in materia.

È il caso, ad esempio, delle richieste di parere sulla liceità della comunicazione di dati dai soggetti pubblici ai privati in relazione alle normative riguardanti l'ordinamento dello *stato civile* e gli *atti anagrafici*, nonché la tenuta delle *liste elettorali*, temi sui quali il Garante si era espresso già nel 1997.

La pronuncia dell'anno precedente, che dichiarava illegittima la prassi di fornire dati ed elenchi delle nascite e dei decessi a terzi al di fuori delle modalità previste dalla normativa in materia di stato civile e di anagrafe, è stata integrata nel 1998 da una nuova decisione riguardante gli elenchi dei nubendi che un Comune era stato richiesto di comunicare sistematicamente agli organi di stampa locali.

Anche in questo caso l'Autorità ha ritenuto che la normativa vigente, che pure permette la diffusione delle singole notizie acquisite caso per caso dall'ufficiale di stato civile, non si presti a una interpretazione estensiva che faccia ritenere lecita la prassi di richiedere al predetto ufficiale di redigere quotidianamente interi elenchi da pubblicare con assiduità.

Analogamente, il Garante ha sottolineato più volte l'impossibilità di procedere alla sistematica divulgazione dei dati anagrafici fuori del caso previsto dal d.P.R. n. 223/1989 (art. 34, comma 1), e cioè nei confronti di altre amministrazioni pubbliche che ne facciano motivata richiesta «per esclusivo uso di pubblica utilità».

Diverso è invece il caso delle liste elettorali, che l'art. 51 del d.P.R. n. 223/1967 assoggetta alla massima divulgazione («chiunque può copiare, stampare o mettere in vendita le liste elettorali del Comune») in una forma tale da non consentire, come ha precisato l'Autorità nel parere reso al Ministero dell'interno il 20 aprile 1998, agli uffici comunali di sindacare le motivazioni alla base delle richieste di accesso.

Pertanto, su questi temi, in tal senso disciplinati dalla normativa vigente, potrebbe essere opportuna una nuova e più coordinata disciplina.

Una parte rilevante dell'attività del Garante nei riguardi del settore pubblico è stata rivolta poi alla soddisfazione di numerose richieste di chiarimenti sui vari adempimenti cui sono soggette le pubbliche amministrazioni. L'Autorità ha precisato ad esempio che i soggetti pubblici, pur non dovendo richiedere il consenso, devono fornire comunque agli interessati l'informativa prevista dall'art. 10 della legge. Tale informativa, è stato peraltro evidenziato, può essere resa adottando modalità semplificate di informazione dei cittadini (ad esempio mediante modelli esplicativi da

esporre o affiggere negli uffici in modo tale, però, da porli in chiara evidenza per il cittadino), specie quando il trattamento dei dati venga effettuato in base a obblighi di legge o di regolamento.

Numerosissimi sono stati poi i quesiti sulle modalità di notificazione dei trattamenti, soprattutto nei primi mesi del 1998, in corrispondenza con i termini del 31 marzo (per i trattamenti svolti anche in parte con l'ausilio di mezzi automatizzati e per i trattamenti di dati sensibili) e del 30 giugno (per i trattamenti non automatizzati). Le pubbliche amministrazioni, infatti, sono state incluse dal d.lg. n. 255/1998 (che ha introdotto nell'art. 7 della l. n. 675/1996 il nuovo comma 5-bis), tra i soggetti che possono effettuare la notificazione in forma semplificata, oltre che esserne del tutto esonerati in determinate ipotesi (comma 5-ter).

Ancora, si è reso necessario specificare ulteriormente, rispetto a quanto già precisato nel 1997, la relazione fra *titolare e responsabile del trattamento* in ambito pubblico, soprattutto in riferimento ai rapporti sempre più fitti fra pubbliche amministrazioni e soggetti privati incaricati di compiere, per le prime, determinate operazioni.

Gli sforzi di semplificare gli adempimenti a carico delle Pa hanno trovato certamente un riscontro nell'atteggiamento di tendenziale attivazione da parte delle amministrazioni stesse per il rispetto della legge. Non possono tuttavia non essere evidenziati alcuni ritardi, ad esempio per quanto riguarda un opportuno monitoraggio dei trattamenti in corso o l'individuazione degli «incaricati» del trattamento.

Già nei primi mesi di applicazione della legge, il Garante si era poi espresso positivamente circa la liceità della scelta da parte di un'amministrazione pubblica di continuare ad avvalersi dei servizi di un soggetto privato nominandolo «responsabile del trattamento» ai sensi dell'art. 8 della l. n. 675/1996.

La validità di tale genere di scelta è stata confermata con una articolata pronuncia del 29 luglio 1998 in materia di accertamenti per il pagamento della tassa sullo smaltimento dei rifiuti solidi urbani. Diversi cittadini e consiglieri comunali si erano infatti rivolti al Garante per ottenere un parere circa la correttezza della prassi adottata dalle amministrazioni comunali di rivolgersi a ditte private per effettuare le misurazioni presso abitazioni private ai fini dell'accertamento della predetta tassa.

L'Autorità, verificata l'esistenza di norme idonee a legittimare in generale tali incarichi (artt. 71 e 73 del d.lg. 15 novembre 1993, n. 507), ha precisato che la concreta responsabilità del trattamento può essere attribuita alla struttura esterna cui è affidata l'attività in convenzione, oppure a un dipendente di quest'ultima, come pure a un ufficio o a un dipendente dell'amministrazione stessa.

Specifiche richieste sono pervenute poi in ordine al concreto esercizio del diritto di accesso ai documenti amministrativi e sulla comunicazione di dati personali ai consiglieri comunali (v. § 2.1.3).

Un altro tema importante sul quale il Garante si è espresso è quello relativo ad alcuni test attitudinali cui un'amministrazione comunale ha sottoposto i propri dipendenti. Interessata dalle locali organizzazioni sindacali, l'Autorità ha rilevato che il modello consegnato ai dipendenti non rispettava alcuni requisiti fondamentali – tra cui l'obbligo di fornire l'informativa – e che alcune risposte ai test consentivano di acquisire informazioni relative alle opinioni politico-sindacali dei lavoratori interessati.

Poiché l'art. 8 dello Statuto dei lavoratori (l. n. 300/1970) reca un esplicito divieto in tal senso, il Garante ha dapprima chiesto elementi di valutazione al Comune, invitandolo a sospendere ogni forma di utilizzazione e ulteriore raccolta dei dati connessi ai test, e successivamente ha imposto, per la prima volta nei confronti di una pubblica amministrazione, il blocco del trattamento dei dati raccolti fino a quel momento.

Sempre nel settore degli enti locali il Garante è intervenuto poi nei confronti dell'ordinanza di un sindaco, adottata in termini analoghi da altre amministrazioni, intesa a fronteggiare il fenomeno della prostituzione attraverso il divieto ai conducenti di autoveicoli di arrestare il proprio mezzo in prossimità di soggetti che si prostituiscono, e di porre in essere altri comportamenti ritenuti di intralcio e di pericolo al traffico stradale.

Tale ordinanza prevedeva anche che, «a tutela della salute pubblica, e in particolare di quella di parenti e affini», si dovesse comunicare al domicilio del trasgressore l'identità di chi avesse violato l'ordinanza, anche nel caso di oblazione.

Il Garante ha eccepito l'illegittimità di questa prescrizione, ritenendo non legittimo che essa fosse disposta con una ordinanza sindacale del genere in esame e giudicando, altresì, privo di corretto fondamento giuridico l'ordine di comunicare la violazione dell'ordinanza al domicilio del contravventore, laddove l'infrazione fosse stata notificata immediatamente sul posto (art. 108, r.d. n. 383/1934).

L'Autorità, poiché l'ordinanza in questione si poneva in contrasto con la legge, anche per ciò che riguardava la sfera di competenza dell'autorità comunale, ha attivato i propri poteri previsti dall'art. 31, comma 1, lett. c) della l. n. 675/1996 e ha invitato l'Amministrazione comunale ad adottare senza ritardo le misure per conformarsi alla segnalazione inviata, appunto, dal Garante.

2.1.2 Trasparenza dell'attività amministrativa

Lo stretto collegamento fra i temi della trasparenza amministrativa e del diritto di accesso ai documenti amministrativi ne consiglia, in questa sede, una trattazione ravvicinata.

Pur nella consapevolezza che il modo più corretto di illustrare l'attività svolta dal Garante in tale materia sia quello di affidarsi a una rassegna dei provvedimenti emanati, sembra opportuno sintetizzare talune premesse generali circa il complesso rapporto tra la pubblicità dell'azione amministrativa e la *privacy* del singolo (o dell'organismo), di volta in volta interessato dall'agire dei pubblici poteri.

Sin dai primi provvedimenti, il Garante ha ricordato che l'art. 43 della l. n. 675/1996 non ha abrogato le precedenti disposizioni che hanno attuato un processo di «apertura» dell'azione amministrativa verso l'esterno. Ci si riferisce, in particolare, all'art. 24, comma 2, lett. d), della l. 7 agosto 1990, n. 241 e all'art. 8, lett. d), del d.P.R. 27 giugno 1992, n. 352, che hanno operato un certo capovolgimento nel rapporto tra segretezza e pubblicità dell'azione amministrativa, nonché all'art. 7 della l. 8 giugno 1990, n. 142, in materia di accesso agli atti dell'amministrazione comunale e provinciale.

Il Garante ha però constatato la tendenza di alcune strutture burocratiche a un sostanziale ritorno verso una «chiusura» della macchina amministrativa, laddove, richiamandosi in maniera inappropriata o pretestuosa la l. n. 675/1996, si sarebbero di fatto mortificate le potenzialità innovative contenute nella normativa sulla trasparenza dell'azione amministrativa.

Più volte, infatti, dinanzi a un assetto normativo che riconosce nella riservatezza un limite all'accesso e al tempo stesso, però, garantisce agli interessati «la visione degli atti relativi ai procedimenti amministrativi la cui conoscenza sia necessaria per curare o difendere i loro interessi giuridici» (art. 24 cit.), il Garante ha richiamato l'attenzione circa la necessità che le singole amministrazioni, sulla base dei criteri stabiliti con i regolamenti adottati ai sensi dell'art. 24, comma 4, della l. n. 241/1990, verifichino di volta in volta la sussistenza delle condizioni per l'esercizio del diritto di accesso e per il corrispondente eventuale sacrificio del diritto alla riservatezza.

Alla luce delle considerazioni qui riassunte, risulta evidente come la mancata abrogazione, da parte della legge in materia di protezione dei dati personali, delle norme tese ad assicurare la trasparenza amministrativa - e in particolare di quelle relative al diritto di accesso ai documenti amministrativi, anche se contenenti dati personali - ha finito con il trasformare il Garante della *privacy* anche in un «Garante della trasparenza», come è stato sottolineato da taluni commentatori.

In altri termini l'Autorità, peraltro in armonia con la giurisprudenza amministrativa (si veda per tutte la decisione dell'Adunanza plenaria del Consiglio di Stato n. 5 del 4 febbraio 1997, in cui è constatata la prevalenza del diritto di accesso sulla riservatezza, laddove questo sia necessario per difendere l'interesse giuridico del richiedente), ha inteso far rispettare la volontà del legislatore del 1996 di non compiere alcun passo indietro lungo il cammino della trasformazione della macchina amministrativa in una «casa di vetro».

Dalle pronunce di seguito citate si ricava, infatti, come il Garante non abbia favorito l'irrigidimento del sistema attraverso una affermazione sistematica della prevalenza del diritto alla riservatezza sul diritto all'informazione. Vi è stata piuttosto un'attenzione costante alle caratteristiche del caso concreto e una opportuna cautela nell'affermazione di principi e regole generali in ordine al contrasto tra riservatezza e accesso ai dati detenuti dalla Pa, qualora questo sia necessario per la cura e la difesa di interessi giuridici alla luce del più volte ricordato art. 24 della l. n. 241/1990. Lo stesso art. 27 della l. n. 675/1996, che consente alla Pa di comunicare e di diffondere dati personali (in particolare quando la comunicazione avvenga verso soggetti privati) solamente se vi è una espressa disposizione di legge o di regolamento che lo consenta, ha costretto il Garante sia a indagare, di volta in volta, la specifica normativa primaria e secondaria di riferimento, sia a osservare trasversalmente uno spettro larghissimo dell'ordinamento.

Già nella *Relazione per l'anno 1997* si è dato conto, oltre che dei principi affermati dalla giurisprudenza amministrativa in materia e del corrispondente orientamento del Garante, del primo provvedimento reso sul tema nell'anno 1998, su richiesta della Presidenza del Consiglio dei ministri, in ordine alla pubblicità della situazione patrimoniale relativa ai titolari di talune cariche elettive e direttive (parere dell'8 gennaio 1998).

Similare è la pronuncia emessa dal Garante in pari data relativamente alla conformità ai principi della l. n. 675/1996 della norma statutaria di un Comune che prevede la pubblicità delle dichiarazioni dei redditi dei consiglieri comunali. L'Autorità si è infatti espressa nel senso di ritenere lecito il regime di pubblicità suddetto, atteso che:

- l'art. 27, comma 3, della l. n. 675/1996 consente ai soggetti pubblici di comunicare e diffondere dati personali a privati o a enti pubblici economici se ciò è previsto espressamente da una norma di legge o di regolamento;
- la normativa statutaria ha, nella gerarchia delle fonti, un rango pari a quello riconosciuto alla normativa regolamentare.

In altra occasione (provvedimento del 30 marzo 1998) il Garante ha poi ravvisato la compatibilità con la l. n. 675/1996 dell'art. 1, comma 8 della l.r. Sicilia 11 maggio 1993, n. 15, che obbliga la regione e gli enti pubblici regionali a comunicare alla presidenza della regione gli incarichi e i compensi corrisposti a ciascun componente privato o pubblico di commissioni, comitati e consigli.

In data 23 gennaio 1998, in risposta alla Corte dei Conti che chiedeva se fossero conformi con i principi della l. n. 675/1996 le rilevazioni che l'Istat deve svolgere nell'ambito del Programma statistico nazionale per il triennio 1998-2000, il Garante ha osservato che poiché l'Istat aveva avviato indagini sulle condizioni di salute e sul ricorso ai servizi sanitari fin dal 1980, il caso poteva rientrare nel regime transitorio

per il trattamento dei dati sensibili di cui all'art. 41, comma 5, della l. n. 675/1996, secondo il quale i trattamenti già iniziati possono essere proseguiti sino al 7 maggio 1998 (termine ora prorogato all'8 maggio 1999 con il d.lg. 6 novembre 1998, n. 389), previa comunicazione al Garante.

Si è inoltre rivolto al Garante il Dipartimento della protezione civile, per conoscere se la SISAM (società privata affidataria della gestione dei velivoli Canadair utilizzati nella lotta agli incendi boschivi) dovesse chiedere il consenso degli interessati per ottemperare alla richiesta proveniente dal medesimo Dipartimento di avere accesso ai nominativi dei piloti impiegati negli anni 1996-97 e all'attività di volo effettuata da ciascuno di essi; ciò in quanto il Dipartimento intendeva esercitare il suo potere ispettivo e di vigilanza sulla predetta società.

Nel caso in esame veniva in considerazione un'ipotesi di comunicazione di dati personali a una pubblica amministrazione da parte di privati e non viceversa, come nelle ipotesi precedenti. In questa occasione il Garante ha ritenuto non necessario il consenso del personale di volo, applicandosi al caso di specie la disposizione dell'art. 20, comma 1, lett. c) della l. n. 675/1996, che esclude il consenso dell'interessato quando il trattamento è effettuato in adempimento di un obbligo previsto da una norma di legge o di regolamento. Tale obbligo è stato infatti rinvenuto nell'art. 6, comma 3, della l. 24 febbraio 1992 n. 225, istitutiva del Servizio nazionale di protezione civile, nonché nel regolamento approvato con d.P.R. 30 gennaio 1993, n. 51, disciplinante le ispezioni al servizio stesso.

Particolare attenzione da parte dell'opinione pubblica si è avuta poi in ordine alla questione sollevata dal Ministero per le politiche agricole, relativa alla possibilità di pubblicare la relazione conclusiva predisposta dalla commissione ministeriale per l'esame dei contratti di circolazione delle quote latte, in cui erano indicate le imprese nei cui confronti sono state rilevate anomalie, nonché i nominativi degli agenti che hanno effettuato gli accertamenti.

La risposta è stata di segno negativo per quanto concerne l'autonoma divulgazione dei dati a terzi da parte del Ministero, mentre è stata ritenuta legittima la comunicazione della relazione al Parlamento, nonché alla Corte dei Conti e alla Procura della Repubblica di Roma per l'eventuale accertamento della sussistenza di una rilevanza di responsabilità amministrativa o penale.

In pari data, il Garante ha peraltro inviato una nota al Presidente del Senato in risposta a una richiesta di parere circa l'utilizzabilità, da parte dei componenti della Commissione IX, dei dati inviati dall'AIMA e di quelli contenuti nella relazione della Commissione governativa di indagine sulle quote latte. Nella circostanza, il Garante ha sottolineato che «il flusso di informazioni nei confronti degli organi parlamentari, anche quando riguarda dati personali, è strumentale al libero esercizio delle funzioni dei singoli componenti della Camera e del Senato, garantite - come ben noto - da puntuali norme costituzionali (artt. 67 e 68, comma 1, della Costituzione)» e che «riguardo ai dati dei quali è prevista la trasmissione al Parlamento una limitazione all'accesso e alla duplicazione da parte dei parlamentari è ammissibile solo in presenza di precise previsioni legislative a tutela dei segreti. Analoga considerazione è stata formulata per quanto concerne l'eventuale diffusione dei dati anche individuali, che poteva derivare dalla stessa pubblicazione dei resoconti delle sedute o di altri atti parlamentari».

Il Garante ha quindi osservato che spetta semmai «al legislatore valutare attentamente, alla luce dei concorrenti principi costituzionali garantiti dalla l. n. 675/1996, quando sia necessario adottare particolari accorgimenti e misure volte a garantire comunque il diritto alla riservatezza degli individui anche rispetto alle prerogative e alle libertà dei componenti del Parlamento».

Il parere dell'Autorità è stato richiesto poi da un Comune relativamente alla possibilità di consegnare a un'impresa commerciale l'elenco di coloro che, a una determinata data, avevano avanzato istanza per il rilascio di concessione edilizia. Il Garante si è espresso in senso negativo, in quanto la normativa urbanistica non prevede tale specifica modalità di comunicazione che comporta un *facere* per l'amministrazione. Nel caso di specie, infatti, l'impresa commerciale chiedeva non tanto di accedere a determinati documenti (come previsto dall'art. 7 della l. 8 giugno 1990, n. 142), quanto piuttosto di ottenere dal Comune l'apposita redazione di uno specifico elenco corredato di particolari indicazioni, volto a documentare atti o documenti distintamente detenuti dall'amministrazione.

Un altro Comune ha chiesto quindi di conoscere se fosse compatibile con la normativa in materia di protezione dei dati personali la legge regionale 4 gennaio 1993, n. 1, del Trentino-Alto Adige, nella parte in cui prevede (artt. 51 e 54) la necessaria pubblicità delle deliberazioni comunali mediante affissione nell'albo pretorio.

Il Garante, dopo aver ricordato che tali norme sono compatibili con l'art. 47 della l. n. 142/1990 che regola la pubblicazione di tutte le deliberazioni comunali e provinciali mediante affissione all'albo pretorio nella sede dell'ente (e che la l. n. 675/1996 non ha abrogato il regime di pubblicità suddetta), ha richiamato l'attenzione sulla necessità che i soggetti privati e gli enti pubblici economici che trattano dati personali rispettino le norme che regolano la conoscibilità e la pubblicità di atti e documenti pubblici (artt. 20, comma 1, lett. *b*), 28, comma 4, lett. *g*) e 43, comma 2 della l. n. 675/1996).

Si è segnalata inoltre l'opportunità che le amministrazioni interessate, qualora le deliberazioni da pubblicare contengano dati «sensibili», selezionino accuratamente - alla luce dei principi di pertinenza e non eccedenza sanciti dall'art. 9 della l. n. 675/1996 - i dati personali la cui inclusione nelle deliberazioni da pubblicare sia realmente necessaria per le finalità proprie di ciascun provvedimento. Si è fatto presente poi che resta fermo, in ogni caso, il divieto di diffondere i dati idonei a rivelare lo stato di salute (art. 23, comma 4 della l. n. 675/1996) nonché, per altro verso, il diritto dei soggetti eventualmente qualificati di accedere ai dati medesimi.

Il Garante, rispondendo poi a un quesito posto dal Dipartimento della funzione pubblica, si è espresso in ordine alla possibilità di diffondere i dati contenuti nella cd. anagrafe dei dipendenti pubblici. Analogamente a quanto già ritenuto nella nota del 23 ottobre 1997 indirizzata al medesimo Dipartimento, la risposta è stata negativa, non essendovi una norma espressa che preveda la diffusione di tali dati. È sembrata tuttavia corretta la prassi adottata dallo stesso Dipartimento di diffondere dati riepilogativi su apposite tabelle statistiche evitando, così, la pubblicizzazione di informazioni di carattere personale.

Di particolare rilievo sono, infine, alcuni provvedimenti sui rapporti tra la l. n. 675/1996 e le normative riguardanti l'ordinamento dello stato civile, gli atti anagrafici e la tenuta delle liste elettorali.

In via generale, il Garante ha segnalato a vari Comuni che la normativa sugli atti anagrafici prevede la possibilità per l'ufficiale dell'anagrafe di rilasciare, anche periodicamente, elenchi di iscritti nell'anagrafe della popolazione residente alle amministrazioni pubbliche che ne facciano richiesta, «per esclusivo uso di pubblica utilità» (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223). Non è prevista, invece, la possibilità di rilasciare tali elenchi ad altri soggetti come privati o associazioni, ai quali i dati anagrafici possono essere comunicati in forma anonima e aggregata, qualora ne sia fatta richiesta per fini statistici e di ricerca e il Comune disponga di idonee apparecchiature (art. 34, comma 2, d.P.R. n. 223/1989).

In particolare, va segnalato invece il parere reso il 20 aprile 1998 in materia di pubblicità delle liste elettorali, al quale si è fatto già cenno (v. § 2.1.1). In esso il Garante diversamente opinando rispetto a quanto ipotizzato dal Ministero dell'interno ha ritenuto che l'art. 51 del d.P.R. n. 223/1967, nella parte in cui stabilisce che «chiunque può copiare, stampare o mettere in vendita le liste elettorali del Comune», non permette «di operare una distinzione tra le finalità per le quali i dati acquisiti attraverso l'accesso alle liste elettorali potrebbero essere successivamente utilizzati», e che «appare difficile sostenere che le finalità di carattere commerciale o pubblicitario eventualmente perseguite dal soggetto che copia la lista non possano essere ricomprese in una norma che consente al privato di vendere le liste stesse e di portare a conoscenza di terzi i dati in esse contenuti». Sicché, allo stato della legislazione vigente, raccogliere e diffondere i dati elettorali non lede di per sé la sfera privata dei cittadini. Tuttavia, chi effettui un tale trattamento dovrà inviare necessariamente ai singoli cittadini interessati l'informativa ex art. 10 della l. n. 675/1996, ponendoli nella condizione di esercitare i diritti stabiliti dall'art. 13 della medesima legge.

Nello stesso parere il Garante ha, infine, rilevato la necessità che i decreti delegati previsti dalla l. n. 676/1996 diano attuazione alla Raccomandazione del Consiglio d'Europa n. R. (91) 10 del 9 settembre 1991, secondo cui la «messa in relazione» dei dati personali provenienti da archivi pubblici accessibili a terzi con altre informazioni raccolte e utilizzate da terzi può essere prevista solo in presenza di «garanzie appropriate».

Va, infine, segnalato il provvedimento sollecitato dal Comune di Trieste, con cui si è constatata l'illegittimità della prassi in uso presso gli uffici dello stato civile di inviare giornalmente ai quondiani locali gli elenchi riportanti i nomi e i cognomi dei nati e dei deceduti nonché le richieste di pubblicazioni di matrimonio. Conformemente a quanto affermato nel precedente parere del 22 luglio 1997, il Garante ha ribadito che non vi è alcuna norma di carattere generale o speciale che consenta all'amministrazione di redigere appositi elenchi da mettere a disposizione di eventuali interessati e che tale forma di comunicazione è pertanto in contrasto con l'art. 27, comma 3, della l. n. 675/1996 (su una fattispecie analoga, si veda anche la recente pronuncia del Consiglio di Stato: Sez. V, 23 gennaio 1998, n. 99; v. anche § 2.1.1). Né vale a sanare l'illegittimità il consenso degli interessati, che è irrilevante nei trattamenti operati dai soggetti pubblici.

Merita da ultimo di essere ricordato il parere del 31 dicembre 1998 relativo alla possibilità, per una azienda sanitaria che intenda effettuare uno *screening* dei tumori, di ottenere dai Comuni gli elenchi anagrafici della popolazione residente e gli eventuali aggiornamenti. Al riguardo il Garante ha constatato la conformità di tali comunicazioni ai principi della l. n. 675/1996 (in particolare dell'art. 27, commi 1 e 2), se si considera che la normativa sugli atti anagrafici consente all'ufficiale dell'anagrafe di rilasciare anche periodicamente gli elenchi suddetti alle amministrazioni pubbliche che ne facciano motivata richiesta «per esclusivo uso di pubblica utilità» (art. 34, comma 1, d.P.R. n. 223/1989).

2.1.3 Diritto di accesso ai documenti amministrativi

Si riferirà ora dei principali provvedimenti emessi dal Garante in materia di accesso ai documenti amministrativi.

In linea generale l'orientamento del Garante è stato quello di ritenere che la l. n. 675/1996 non abbia introdotto un regime di assoluta riservatezza dei dati e che si debba verificare caso per caso l'esistenza di altri diritti o interessi di pari o superiore tutela. Tra tali diritti, si è detto, rientra sicuramente l'accesso ai documenti am-

ministrativi, che è tuttavia riconosciuto solo a chi sia titolare di un interesse personale e concreto in relazione alla tutela di situazioni giuridicamente rilevanti (art. 22, l. n. 241/1990; art. 2, d.P.R. n. 352/1992).

L'aspetto che merita maggiormente di essere sottolineato è che la sussistenza di tale diritto nei casi concreti deve essere ravvisata dalla stessa amministrazione nei cui confronti l'interessato eserciti il diritto di accesso, anziché, a posteriori, dal Garante. L'Autorità può semmai intervenire, in via preventiva o successiva, per fornire chiarimenti o quando il dato sia stato (o stia per essere) comunicato o diffuso oltre l'ambito consentito dall'esercizio del diritto di accesso. Sicché il sistema ha finito con il confermare gli ambiti delle rispettive competenze: quella delle singole amministrazioni da un lato e quella del Garante dall'altro.

Tale ripartizione emerge implicitamente da un provvedimento del 23 gennaio 1998, in riferimento a un caso nel quale un membro della Camera dei deputati aveva chiesto chiarimenti circa il rifiuto frapposto dal Dipartimento dello spettacolo a una sua richiesta di accesso ai documenti relativi a determinate erogazioni di contributi e ai relativi verbali. Al riguardo il Garante, constatato che il Dipartimento aveva negato l'esistenza di un interesse giuridicamente rilevante all'accesso (e che un decreto ministeriale precludeva la divulgazione dei verbali delle commissioni in favore di soggetti «diversi da quelli direttamente contemplati nella deliberazione»), ha osservato che:

- il limite alla conoscibilità di quei documenti deriva non tanto dalla l. n. 675/1996 quanto dalla specifica disciplina sull'accesso ai documenti amministrativi e dalla conoscibilità dei verbali delle commissioni prevista dal citato decreto ministeriale;

- compete al Dipartimento dello spettacolo valutare se le esigenze di studio delle problematiche dello spettacolo da parte di un parlamentare possano essere considerate alla stregua di un «interesse giuridicamente rilevante» e che tale valutazione è eventualmente sindacabile in sede giurisdizionale;

- l'art. 8 del d.lg. 8 gennaio 1998, n. 3, riguardante il riordino degli organi collegiali operanti presso il Dipartimento dello spettacolo, prevedendo la costituzione di nuove commissioni nel settore, ha aperto la possibilità di eventuali modifiche anche nella disciplina dell'attività svolta in materia dal Dipartimento;

- ciascun parlamentare ha comunque la possibilità di esercitare in altro modo le proprie prerogative presentando, in particolare, ulteriori interrogazioni e interpellanze a cui il Governo dovrebbe fornire sollecita risposta.

Numerose sono state poi le richieste di chiarimenti da parte di amministrazioni (e singoli consiglieri) comunali e provinciali circa l'esistenza e i limiti del diritto dei consiglieri comunali e provinciali di ottenere dagli uffici dell'ente informazioni utili per l'espletamento del proprio mandato.

Con un parere del 20 maggio 1998 il Garante, dopo aver ribadito che l'art. 31, comma 5 della l. n. 142/1990 riconosce ai consiglieri il diritto a ottenere «notizie e informazioni utili all'espletamento del proprio mandato», ha osservato che:

- il consigliere comunale e provinciale, se invoca il cit. art. 31, non deve dimostrare l'esistenza di un interesse giuridicamente rilevante, essendo sufficiente che rappresenti l'utilità delle notizie e delle informazioni richieste rispetto al mandato; l'amministrazione, dal canto suo, deve rispettare il principio di pertinenza di cui all'art. 9, comma 1, lett. d), della l. n. 675/1996 rispetto alle notizie e alle informazioni fornite;

- in presenza della dichiarazione da parte del consigliere di avvalersi della facoltà di cui all'art. 31 della l. n. 142/1990, sarebbe arbitraria, da parte dell'amministrazione, una distinzione basata sulla natura dei dati richiesti;

– l'art. 31, tuttavia, deve essere coordinato con altre norme vigenti che tutelano il segreto delle indagini penali o la segretezza della corrispondenza;

– il diritto di accesso deve essere parimenti coordinato con la speciale disciplina relativa agli atti anagrafici, allo stato civile e alle liste elettorali.

Va segnalato anche il provvedimento del 29 maggio 1998, in riferimento a un quesito con cui l'Azienda Municipale Ambiente (AMA) di Roma aveva chiesto di verificare la possibilità di comunicare i nominativi dei dipendenti preposti alle proprie sedi territoriali a un consigliere del Comune che ne aveva fatto richiesta. La risposta è stata positiva, in quanto l'art. 31 della l. n. 142/1990 prevede espressamente che il consigliere comunale ha il diritto di acquisire notizie utili al proprio mandato, anche se relative a enti strumentali del Comune per la gestione di servizi pubblici, quale l'AMA. Considerato quindi che la giurisprudenza della Cassazione ha riconosciuto che le aziende speciali hanno natura di enti pubblici economici (e ricordato che la normativa in materia di protezione dei dati personali assoggetta questi ultimi al regime «ordinario» previsto per i soggetti privati), il Garante ha ritenuto che l'AMA potesse effettuare la suddetta comunicazione in virtù dell'art. 20, comma 1, lettera c) della l. n. 675/1996, la quale esime gli enti pubblici economici dal richiedere il consenso dell'interessato nel caso in cui, come quello di specie, il trattamento doveva essere effettuato in adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria.

Di contenuto praticamente identico al parere reso all'AMA è poi quello del 10 giugno 1998, in cui l'Azienda servizi pubblici del Comune di Brandolo di Chioggia ha posto analogo quesito. In materia di appalti il Garante ha formulato quindi diversi pareri per il cui contenuto si rinvia al § 2.1.10.

Si segnala inoltre il provvedimento del 3 settembre 1998 con cui il Garante, a fronte di una richiesta della Camera di commercio di Treviso di chiarire se fosse necessario il consenso per comunicare dati relativi a procedure di gara per appalti d'opera o di fornitura, ha ribadito come la «riservatezza» delle società partecipanti a una gara sia stata presa già in considerazione da leggi anteriori alla l. n. 675/1996 (art. 14, comma 3, d.lg. n. 358/1992 e 14, comma 3, d.lg. n. 157/1995), nelle parti in cui prevedono che si possano chiedere informazioni non eccedenti l'oggetto dell'appalto e che vadano però tenuti in considerazione «gli interessi legittimi del concorrente relativi alla protezione di interessi tecnici e commerciali». Sicché, nel caso di specie, l'accesso è stato ritenuto possibile.

Va, infine, segnalato il caso del Comune di Marradi che aveva fornito alla cooperativa che gestisce una comunità terapeutica l'elenco dei sottoscrittori di una petizione tesa a migliorare i rapporti tra i cittadini e gli ospiti della comunità medesima.

In tale parere il Garante, dopo avere ribadito che la normativa sulla trasparenza e la partecipazione del cittadino al procedimento amministrativo non è stata abrogata e che l'amministrazione è legittimata essa stessa a stabilire se il diritto di accesso debba trovare o no soddisfazione dei singoli casi, ha segnalato l'incertezza interpretativa che si riscontra anche nella giurisprudenza amministrativa sul rapporto tra l'art. 7 della l. n. 142/1990 e l'art. 22 della l. n. 241/1990 (ci si chiede infatti se la prima norma abbia una portata più ampia rispetto alla seconda, rendendo superflua la dimostrazione da parte del richiedente di un interesse giuridicamente rilevante per l'accesso).

Il Garante ha precisato, altresì, come le norme sull'accesso ai documenti amministrativi non rechino parametri dettagliati per tutelare in concreto il diritto alla riservatezza. Dopo aver evidenziato come il grado di tutela della riservatezza sia comunque aumentato dopo la l. n. 675/1996, specie in materia di dati sensibili, ha però ipotizzato ulteriori interventi normativi per offrire alle amministrazioni destina-

tarie delle richieste di accesso, elementi di valutazione più concreti, elementi che potrebbero ridurre sia le incertezze constatate, sia alcune difformità che si registrano oggi rispetto alle decisioni assunte sul diritto di accesso. E ha concluso nel senso che istanze, petizioni e proposte debbano essere ritenute di per sé pubbliche, unitamente ai dati relativi ai promotori e sottoscrittori.

2.1.4 Dati sensibili utilizzati dalla pubblica amministrazione

Nel corso dell'anno di attività, la risoluzione delle problematiche riguardanti il trattamento dei dati sensibili da parte delle pubbliche amministrazioni è stata fortemente caratterizzata dalle proroghe del regime transitorio previsto dall'art. 41, comma 5 della l. 31 dicembre 1996, n. 675.

Come è noto, in armonia con la direttiva comunitaria, la l. n. 675/1996 stabilisce un particolare regime per i trattamenti che coinvolgono dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché lo stato di salute e la vita sessuale, imponendo per tali dati, definiti appunto «sensibili», una maggiore trasparenza sulle modalità di trattamento.

Per i trattamenti effettuati da soggetti pubblici, tale garanzia sarà integrata, a regime, dall'integrale attuazione del principio di riserva di legge sancito dall'art. 22, comma 3 della l. n. 675/1996.

La norma, rafforzando il principio di finalità stabilito per i soggetti pubblici in merito al trattamento dei dati personali «comuni» (art. 27, comma 1), circoscrive la tipologia dei trattamenti possibili in materia di dati sensibili, nonché la fonte del relativo potere, individuandola esclusivamente in una apposita disposizione di legge nella quale siano indicati «i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite».

Il regime transitorio è previsto dall'art. 41, comma 5 al fine di permettere alle amministrazioni, in tutti i casi in cui non si riscontri una norma di legge che presenti i requisiti suddetti, di proseguire i trattamenti di dati «sensibili» in corso fino all'8 maggio 1999, previa comunicazione a questa Autorità, nelle more dell'approvazione di specifiche leggi.

Si segnala tuttavia che l'attività normativa in materia si è rivelata particolarmente complessa e che ciò ha spiegato una certa influenza sugli slittamenti che sono stati disposti rispetto al termine inizialmente previsto. La prima scadenza è stata prorogata una prima volta all'8 novembre 1998 (dall'art. 1 del d.lg n. 135/98) e poi all'8 maggio 1999 (dall'art. 1 del d.lg 6 novembre 1998, n. 389), sicché, come si è detto, il regime transitorio ha finito per costituire nel corso dell'anno il principale quadro normativo di riferimento per il trattamento dei dati sensibili.

Lo schema del decreto legislativo per il trattamento dei dati sensibili da parte dei soggetti pubblici, approvato dal Consiglio dei ministri il 22 luglio 1998 ma non emanato, è stato superato di fatto dal d.lg. 6 novembre 1998, n. 389, che ha differito nuovamente all'8 maggio 1999 il termine finale del regime transitorio più volte citato.

Nelle more, quindi, dell'emanazione dei provvedimenti legislativi riguardanti specificatamente la disciplina dei dati sensibili da parte dei soggetti pubblici, questa Autorità si è impegnata per una maggiore diffusione della conoscenza - e applicazione - delle disposizioni della legge in merito a tali ambiti di trattamenti, curando anche la pubblicazione di provvedimenti di carattere generale che riassumessero i numerosi quesiti e istanze che sono stati formulati in materia.

A tale proposito si richiama in primo luogo il provvedimento del 13 febbraio 1998, con il quale il Garante è tornato sulle problematiche relative al settore della sanità già affrontate nella nota del 30 giugno 1997, e in particolare sulla illustrazione delle diverse modalità del trattamento che devono essere osservate da medici, farmacisti, esercenti le professioni sanitarie e organismi sanitari pubblici. Con questo provvedimento sono stati forniti chiarimenti in ordine ai contenuti delle certificazioni mediche e ad alcune modalità semplificate per l'applicazione della l. n. 675/1996, evidenziando talune misure temporanee di carattere organizzativo che le amministrazioni del settore della sanità sono tenute a osservare al fine di tutelare l'anonimato dei pazienti nelle procedure amministrative connesse ai trattamenti sanitari.

In altre occasioni, sempre con provvedimenti di carattere generale o suscettibili di risolvere delicate questioni di principio, l'Autorità è intervenuta per chiarire la portata delle altre disposizioni della l. n. 675/1996 in materia di dati sensibili.

Rilevante, a questo proposito, è il parere del 29 maggio 1998 reso alle Ferrovie dello Stato Spa in ordine alla definizione del regime applicabile alle società nate dalla privatizzazione di enti pubblici. In questa occasione il Garante ha chiarito che, data la natura privata delle Ferrovie dello Stato Spa (società per azioni derivante dalla trasformazione dell'Ente Ferrovie dello Stato), la normativa di riferimento per il trattamento dei dati relativi allo stato di salute dei dipendenti deve rinvenirsi nell'art. 22, comma 1 della l. n. 675/1996.

Si segnala inoltre il parere del 5 agosto 1998 con il quale sono stati forniti alcuni chiarimenti al Ministero dell'università e della ricerca scientifica e tecnologica che chiedeva di conoscere se i dati relativi alle preiscrizioni alle università, effettuate ai sensi dell'art. 3 del d.m. 21 luglio 1997, n. 245, abbiano o no natura sensibile. Al riguardo il Garante ha osservato che alcuni dati contenuti nel modulo informatico previsto dal d.m. 23 aprile 1998 - quali ad esempio quelli relativi agli ausili personalizzati - rivestono senz'altro natura sensibile e che, in quanto tali, possono essere trattati dalle università e dalle scuole pubbliche fino alla scadenza del termine transitorio dell'8 maggio 1999.

Si è inoltre rilevato che la trasmissione di elenchi di studenti da parte del MURST verso altri soggetti (scuole, università, regioni), è attualmente regolata dal solo d.m. 23 aprile 1998 anziché da una norma di rango legislativo o regolamentare. Si è suggerito pertanto di integrare il citato d.m. 21 luglio 1997, n. 245, al fine di regolare il flusso di dati verso altri soggetti pubblici e privati ai sensi dell'art. 27, commi 2 e 3 della l. n. 675/1996.

Talora il Garante ha avuto modo di pronunciarsi su richiesta del Governo, nell'ambito delle proprie attribuzioni consultive. Particolarmente rilevante è stata l'attività svolta in occasione della conversione del cd. «decreto-legge Di Bella» (d.l. 17 febbraio 1998, n. 23).

L'art. 5 di tale d.l., come modificato dalla legge di conversione 8 aprile 1998, n. 94, stabilisce che le prescrizioni mediche devono contenere non l'indicazione delle generalità del paziente, ma «un riferimento numerico o alfanumerico di collegamento a dati d'archivio in proprio possesso che consenta, in caso di richiesta da parte dell'autorità sanitaria, di risalire all'identità del paziente trattato». L'art. 5-bis del medesimo d.l., inserito dalla citata legge, disciplina inoltre il profilo del consenso del paziente al trattamento sanitario e demanda al Ministero della sanità e alle aziende sanitarie locali l'individuazione delle procedure dirette ad assicurare che le ricette siano esaminate dal solo personale competente incaricato di svolgere verifiche amministrative e a scopi epidemiologici e di ricerca.

Tali disposizioni sono state emanate recependo alcune delle osservazioni formulate da questa Autorità alla presidenza della Commissione igiene e sanità del Senato, nelle quali si poneva particolare attenzione alla necessità di un alto livello di definizione della norma che avrebbe disciplinato i limiti di utilizzazione dei dati sanitari, con l'indicazione appunto delle amministrazioni alle quali i dati saranno trasmessi e delle finalità della trasmissione.

In altra materia concernente la delega conferita al Governo dall'art. 59, commi 50 e 51, della l. 27 dicembre 1997, n. 449, di accompagnamento alla legge finanziaria, il problema dei dati sensibili è emerso nel senso della necessità, evidenziata dal Garante in sede di parere, di assicurare la idonea tutela di tali informazioni in ambiti in cui il diritto alla *privacy* si trova di fronte all'interesse dello Stato alla regolarità ed efficienza dei pubblici servizi e delle pubbliche entrate a essi connesse.

La citata legge, come è noto, ha delegato il Governo (art. 59, comma 51) a individuare criteri unificati per la valutazione della situazione economica di cittadini che intendano usufruire di prestazioni sociali agevolate in ambito pubblico (cd. «riccometro»), nonché a definire le procedure per l'acquisizione delle informazioni (v. § 2.1.8).

Una ulteriore delega (art. 59, comma 50) riguardava le disposizioni per il riordino della partecipazione alla spesa sanitaria e delle relative esenzioni (cd. «sanitometro», v. § 2.1.8).

A tale riguardo, con le note rese alla Presidenza del Consiglio dei ministri, rispettivamente il 26 marzo 1998 e il 20 aprile 1998, il Garante ha formulato osservazioni in merito alle disposizioni dello schema dei decreti legislativi relativi al «riccometro» e al «sanitometro». Le note hanno precisato le modifiche che avrebbero dovuto essere apportate ai decreti al fine di renderli in linea con le disposizioni della l. n. 675/1996, e hanno ribadito la necessità di rispettare il criterio generale previsto dall'art. 22, comma 3 della legge, che individua la garanzia del trattamento dei dati sensibili non già nel consenso dell'interessato, bensì in una norma di rango primario indicativa delle finalità perseguite e delle operazioni effettuabili.

Tali modifiche sono state recepite solo in parte (v. § 2.1.8).

2.1.5 Documenti elettronici e carte magnetiche

Il progresso tecnologico registrato negli ultimi anni nel campo delle comunicazioni informatiche e telematiche ha comportato la messa a punto, anche nella pubblica amministrazione, di vari progetti per l'introduzione di documenti elettronici e carte magnetiche destinati a sostituire gli attuali modelli cartacei utilizzati per identificare le persone o a condensare in un unico supporto alcune informazioni di più frequente utilizzazione e che possono rivelarsi utili per semplificare il rapporto tra il cittadino e la pubblica amministrazione.

La creazione di tali documenti richiede, però, alcune garanzie non solo di sicurezza e di integrità dei dati, ma, soprattutto, di corretta utilizzazione delle informazioni personali, prestando particolare attenzione ai dati sanitari e ai soggetti legittimati ad accedervi.

Assumono particolare interesse, in tale ambito, la carta d'identità e gli altri documenti di riconoscimento «elettronici» (cioè rilasciati con strumenti informatici) previsti dalla l. 16 giugno 1998, n. 191 (cd. «Bassanini-ter»).

L'individuazione delle caratteristiche e delle modalità di rilascio di tali documenti è demandata a un regolamento governativo sul cui schema il Garante ha recentemente espresso le proprie valutazioni, ai sensi dell'art. 31, comma 2, della l. n. 675/1996 (v. § 3.1.3).

Con tale parere il Garante, nell'esprimere ampia considerazione per le finalità di semplificazione dell'attività amministrativa perseguite dal provvedimento, ha ritenuto, in uno spirito di collaborazione, di formulare alcune considerazioni volte ad assicurare una piena armonia del testo con i principi in materia di tutela dei dati personali.

In particolare, il Garante ha rappresentato l'esigenza di una maggiore chiarezza del testo in ordine all'eventuale introduzione di un «codice individuale» che potrebbe rappresentare un nuovo strumento di identificazione delle persone utilizzabile in termini universali, anche per fini diversi da quello fiscale. Il Garante ha evidenziato che lo schema meritava alcune precisazioni al riguardo, tenuto conto che l'eventuale introduzione di un nuovo codice di identificazione personale:

- risulterebbe in contrasto con la citata l. n. 191/1998 che fa espresso riferimento al solo codice fiscale;
- richiederebbe una norma primaria recante precise garanzie in ordine ai presupposti e alle condizioni per la sua utilizzazione, in conformità al diritto comunitario (art. 8, par. 7, della direttiva 46/95/CE) e all'espresso criterio di delega contenuto nella l. n. 676/1996 (art. 1, comma 1, lett. d)).

Inoltre, poiché fra i dati da inserire nella carta d'identità elettronica la l. n. 191 prevede anche taluni «dati sanitari» del cittadino, il Garante ha sottolineato il rischio di una proliferazione o sovrapposizione di documenti elettronici contenenti dati inerenti alla salute e più precisamente di una sovrapposizione con la disciplina della tessera sanitaria prevista dalla l. n. 449/1997 la cui adozione in via sperimentale è stata recentemente finanziata dal d.l. 28 dicembre 1998, n. 450, convertito dalla l. 26 febbraio 1999, n. 39 (v. § 2.6.4).

Questa esigenza di armonizzazione e di garanzie per il cittadino ricorre, ovviamente, anche per altri documenti elettronici di cui è ipotizzata l'introduzione (ad esempio, per il libretto di lavoro).

2.1.6 Rete unitaria della pubblica amministrazione

Il Garante ha continuato a seguire attentamente i progressi che si registrano nella realizzazione della Rete unitaria della pubblica amministrazione, la quale, nell'ambito di un complesso processo di trasformazione dell'apparato statale, dovrebbe condurre nel breve termine a una più ampia automazione dei servizi e alla progressiva informatizzazione degli uffici.

Già nella precedente *Relazione per l'anno 1997* il Garante aveva sottolineato l'esigenza che la gestione informatica dei flussi documentali, che consentirà l'interscambio dei dati tra numerose amministrazioni e verso i cittadini, potrà svilupparsi efficacemente solo se, al contempo, verrà tracciato un preciso quadro di garanzie per ciò che riguarda il rispetto di alcune garanzie che riguardano, in primo luogo, la compatibilità tra le finalità perseguite dalle varie amministrazioni interessate e la pertinenza e non eccedenza dei dati raccolti.

Nel corso del 1998 il Garante ha richiamato l'attenzione su questi temi in occasione dei numerosi provvedimenti adottati in tema di comunicazione di dati tra pubbliche amministrazioni. Ha sviluppato poi precise riflessioni espresse nei primi mesi del 1999, anche in assenza della prescritta richiesta, nei pareri, a proposito degli schemi di regolamento sul documento d'identità elettronico, sull'accesso ai centri storici e alle zone a traffico limitato, nonché sull'interscambio di dati fra anagrafi.

Non è stato invece possibile, a causa della mancata consultazione del Garante, formulare osservazioni e proposte in altre occasioni, in particolare per ciò che riguarda lo schema di d.P.R. sulla gestione del protocollo informatico da parte delle amministrazioni pubbliche (d.P.R. 20 ottobre 1998, n. 428, che pure menziona erroneamente il Garante tra le autorità consultate), e lo schema di d.P.R. sul telelavoro nelle pubbliche amministrazioni (d.P.R. 8 marzo 1999, n. 70).

Per quanto riguarda, invece, il citato argomento dell'interscambio anagrafico, il Garante ha affrontato i delicati problemi scaturiti dall'emanazione della circolare 1° dicembre 1998, n. MIACEL n. 20 del Ministero dell'interno con la quale, nell'ambito dell'attivazione del sistema di accesso e interscambio anagrafico, è stata portata a conoscenza, mediante pubblicazione nella «Gazzetta Ufficiale», la convenzione stipulata fra la stessa amministrazione dell'interno e l'ANCI.

In una nota del 4 marzo 1999 diretta al Ministro dell'interno, il Garante ha comunicato di aver appreso solo dalla «Gazzetta Ufficiale» che l'Amministrazione dell'interno ha aderito a un articolato progetto per l'attivazione di un complesso sistema di interconnessione telematica che coinvolgerebbe, in primo luogo, le anagrafi comunali, nonché le banche dati di alcuni enti pubblici.

Il Garante ha manifestato sorpresa nell'apprendere che una iniziativa così importante e significativa, e che incide profondamente sul sistema di comunicazione ad altri enti pubblici dei dati personali contenuti nelle anagrafi comunali, sia stata adottata senza coinvolgere l'Autorità stessa, cui la l. n. 675/1996 assegna una sicura competenza in materia; ha pertanto manifestato il proprio disappunto per la mancata consultazione disciplinata dall'art. 31, comma 2, della cit. l. n. 675/1996.

Il Garante ha constatato poi che la convenzione tra il Ministero dell'interno e l'ANCI contiene in più parti alcuni riferimenti al Garante senza che l'Autorità stessa sia stata in alcun modo coinvolta nei lavori preparatori, né tantomeno indicata tra i destinatari per conoscenza della circolare medesima.

In particolare, si è rilevato addirittura che questa Autorità è stata espressamente coinvolta in più punti della convenzione per fornire «indicazioni» ai fini della vigilanza sull'adeguamento tecnologico e procedurale del servizio di interconnessione o per la partecipazione in un gruppo stabile per il coordinamento, il controllo e la valutazione della fase di avvio (art. 4 e allegato della convenzione stipulata con l'ANCI il 9 luglio 1998, allegata alla circolare 1° dicembre 1998, n. MIACEL 20).

Nel merito del provvedimento, al di là dei vari aspetti certamente positivi che l'iniziativa assume in vista della semplificazione burocratica e della riduzione dei costi dei servizi pubblici, l'Autorità ha rilevato che l'ipotizzato processo di interconnessione delle anagrafi comunali determina un impatto significativo nel sistema di circolazione dei dati in atto nell'ambito della pubblica amministrazione, che doveva essere valutato meglio alla luce dei principi sanciti in materia di protezione dei dati personali, specie nella parte in cui si prevede la possibilità di interscambio tra comuni e tra questi e le altre pubbliche amministrazioni.

In particolare, si è osservato, la trasformazione del codice fiscale in un codice individuale richiede una particolare base normativa che era stata già evidenziata nel parere del Garante reso sullo schema di d.P.R. in materia di documento d'identità elettronico.

Analoga osservazione è stata fatta a proposito della sostanziale introduzione di una «anagrafe delle anagrafi», il cui impatto è di tutta evidenza meritevole di seri approfondimenti per ciò che riguarda la tutela dei dati personali.

Come si è già ricordato, infatti, la disciplina delle modalità di utilizzo delle banche dati pubbliche da parte delle varie amministrazioni deve essere contenuta in norme di legge o di regolamento, in conformità alle condizioni previste dall'art. 27 della l. n. 675/1996, al fine di realizzare un flusso di dati trasparente e ispirato a criteri omogenei che garantiscano la protezione dei dati nel rispetto dei principi di pertinenza, completezza e non eccedenza sanciti dall'art. 9, lett. d) della medesima l. n. 675/1996.

Questa Autorità ha auspicato, in conclusione, una approfondita riflessione sull'argomento, restando a disposizione per ogni opportuno contributo in relazione ai successivi provvedimenti che il Ministero intenderà adottare al riguardo, volti a disciplinare il trattamento dei dati personali nell'ambito della pubblica amministrazione, nel rispetto della normativa in tema di accesso e di tutela della riservatezza, con predisposizione, anche in sede tecnica, di apposite misure e procedure per la salvaguardia dei dati protetti.

2.1.7 Notificazione di atti giudiziari e amministrativi

In oltre 70 segnalazioni alcuni interessati (persone fisiche e giuridiche) hanno lamentato che vari atti provenienti da (o diretti a) uffici giudiziari e da altri organi competenti, specie in materia fiscale o di circolazione stradale, sono notificati a terzi (quali portieri o vicini di casa) o pubblicati, anche per estratto, a mezzo stampa.

È stata pertanto affrontata la questione del rapporto tra le esigenze di pubblicità o di certezza della conoscenza degli atti e il diritto degli interessati di non subire una ingiustificata divulgazione dei propri dati personali.

Al riguardo il Garante ha rilevato che la l. n. 675/1996 non ha abrogato né le disposizioni in materia di notificazioni di atti contenute nel codice di procedura civile (o da questo mutate) che consentono di rilasciare una copia leggibile di atti o un loro estratto a terzi, né le norme relative alla formazione e comunicazione degli atti del processo penale.

Le notificazioni di tali atti a persone diverse dagli interessati sono state quindi ritenute legittime, in termini generali, perché conformi alle norme applicabili.

L'Autorità, come aveva fatto in precedenza con il Ministero di grazia e giustizia, ha invitato le competenti amministrazioni - anche con riferimento all'art. 1, comma 1, lett. i) della l. n. 676/1996, che prevede l'emanazione di norme delegate in materia - a proporre modifiche della vigente normativa, e ha altresì indicato alcune cautele idonee a ridurre i problemi evidenziati nelle more delle predette modifiche. Ciò in applicazione dei vincolanti principi di correttezza del trattamento e di pertinenza dei dati trattati, sanciti dall'art. 9 della l. n. 675/1996, anche in riferimento alla Convenzione n. 108/1981 del Consiglio d'Europa.

In particolare è stata anzitutto rappresentata l'opportunità che il giudice civile eserciti con maggiore frequenza il potere di prescrivere, anche d'ufficio, forme particolari di notificazione «quando lo consigliano circostanze particolari» (art. 151, c.p.c.).

In secondo luogo, considerato che la busta chiusa che contiene l'atto da notificare per posta reca un numero limitato di dati (art. 3, l. n. 890/1982), è stato raccomandato un ricorso più ampio al servizio postale, salvi i divieti espressi di legge o i casi in cui la notificazione debba essere eseguita personalmente (art. 149, c.p.c. art. 1, l. 20 novembre 1982, n. 890).

In terzo luogo si è auspicato che l'ufficiale giudiziario, benché le attuali norme del codice non lo impongano, consegna in busta chiusa la copia dell'atto qualora la consegna avvenga a persona diversa da quella indicata nell'atto stesso.

L'applicabilità delle disposizioni del codice di procedura civile è stata rilevata anche:

- per gli atti del processo amministrativo notificati ai sensi degli artt. 3 e segg. del regolamento di procedura del Consiglio di Stato (r.d. 17 agosto 1907, n. 642);
- per gli atti provenienti da uffici fiscali (art. 60 del d.P.R. n. 600/1973) e per i verbali relativi a contravvenzioni al codice stradale (art. 201 del d.lg. n. 285/1992);
- per le ingiunzioni e i verbali relativi ad altri illeciti amministrativi e alle relative sanzioni pecuniarie (art. 14 della l. n. 689/1981).

Per le contravvenzioni per eccesso di velocità si è poi osservato che le norme prevedono la notificazione del verbale di violazione (art. 201, d.lg. n. 285/1992 e art. 384, d.P.R. n. 495/1992), ma non anche della fotografia, che può essere semmai richiesta dal destinatario del verbale.

È stato chiarito anche che rientra non nella competenza del Garante, ma in quella di autorità giudiziarie e amministrative, esaminare i vizi e le irregolarità della notificazione asseriti dall'interessato, nei limiti consentiti dalla rilevanza giuridica della relazione di notificazione (v. art. 148, c.p.c. e artt. 2699 e 2700 c.c.).

Si è chiarito ancora che il notificatario può indicare agli uffici tributari chi sia il vero debitore del tributo, sia perché il trattamento di dati per scopi personali non è soggetto alla l. n. 675/1996 benché si proceda a una comunicazione episodica di dati (art. 3), sia perché la comunicazione dei dati è ammessa per tutelare i propri diritti in sede giudiziaria (art. 20, comma 1, lett. g)).

Per quanto riguarda poi gli atti conclusivi del procedimento penale - in particolare l'avviso all'imputato contumace del deposito in cancelleria della sentenza, nonché il decreto penale emesso ex artt. 459 ss., c.p.p. - si è rilevato che questi, essendo atti pubblici, possono essere rilasciati a persone estranee e, quando la legge lo preveda, pubblicati sui giornali.

Quanto alle notificazioni dirette alla persona offesa dal reato, si è osservato che il codice non prevede che esse siano effettuate in plico chiuso (art. 154, comma 1).

Per l'invio da parte del giudice per le indagini preliminari a un minorenne dell'avviso di convocazione notificato aperto e leggibile al portiere dello stabile dell'interessato, si è rilevata invece l'applicabilità delle comuni forme di notificazione. Ciò sebbene l'art. 13, comma 1, del d.P.R. n. 448/1988 vieti la pubblicazione e la divulgazione, con qualsiasi mezzo, di notizie o immagini idonee a consentire l'identificazione del minorenne comunque coinvolto nel procedimento, e benché l'art. 16 della Convenzione ONU di New York del 20 novembre 1989 sui diritti del fanciullo, ratificata con l. n. 176/1991, sancisca il diritto del minore alla protezione «contro interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza».

Si è segnalata anche qui l'esigenza che gli atti notificati a persone diverse dai destinatari in essi indicati siano chiusi in busta.

Rispetto ai certificati elettorali, consegnati spesso dagli incaricati a vicini di casa, non si è ravvisata lesione alla riservatezza degli interessati, in quanto essi recano dati accessibili a chiunque ai sensi dell'art. 51 del d.P.R. n. 223/1967.

Per le sentenze emesse in materia di rettificazione di attribuzione di sesso si è ritenuta applicabile, in mancanza di diversa disposizione, la regola generale sulla pubblicità delle sentenze (art. 133, c.p.c.). Questo benché le conseguenti attestazioni di stato civile riferite alla persona, della quale sia stata giudizialmente rettificata l'attribuzione di sesso, debbano essere rilasciate con la sola indicazione del nuovo sesso e nome (art. 5, l. 14 aprile 1982, n. 164).

Circa l'invio al luogo di lavoro dell'interessato di un atto giudiziario a lui diretto, si è osservato che le norme del codice di procedura civile consentono la notificazione nel luogo in cui il destinatario «ha l'ufficio o esercita l'industria o il commercio» (artt. 138 e 139 c.p.c.).

Il Garante ha suggerito agli interessati di rivolgere direttamente al titolare del trattamento la richiesta di conoscere come l'organo notificante abbia ottenuto l'indirizzo del luogo di lavoro, specificando che nei confronti dell'ufficiale giudiziario il diritto di conoscere l'origine dei dati può essere esercitato, semmai, per il tramite di un eventuale accertamento del Garante (art. 32, comma 6). Nei confronti di altri soggetti, invece, si è ricordato che il Garante può essere adito qualora il diritto di accesso sia da essi illegittimamente negato (v. artt. 14, comma 1, lett. *e*) e 12, lett. *h*) della l. n. 675/1996) o non trovi adeguata soddisfazione.

Circa la trattazione pubblica delle cause civili riguardanti il diritto di famiglia e lo stato delle persone, si è poi osservato che la regola generale della pubblicità, a pena di nullità, delle udienze di discussione (art. 128, c.p.c.), assicura la trasparenza dell'amministrazione della giustizia e si collega all'art. 101 della Costituzione; che la scelta tra l'udienza pubblica e la camera di consiglio è operata direttamente dal codice in relazione al tipo di controversia, e che lo stesso art. 128, c.p.c. prevede la possibilità per il giudice di disporre, per determinate ragioni, che l'udienza si svolga a porte chiuse.

Si è anche rilevato che in alcuni casi la conoscenza del contenuto degli atti da parte di terzi può risultare lesiva della dignità dell'interessato, che potrebbe essere indotto a modificare per ciò stesso la propria strategia difensiva, o a sopassedere all'esercizio dei propri diritti. Le auspiccate modifiche normative saranno quindi utili anche per prevenire censure che potrebbero essere eventualmente mosse in sede giurisdizionale in riferimento agli artt. 24 e 3 della Costituzione.

In questo contesto l'emanazione della l. 28 settembre 1998, n. 337, che ha delegato il Governo a emanare, entro sei mesi dalla sua entrata in vigore, disposizioni (eventualmente da rivedere o correggere entro due anni dalla loro entrata in vigore) in materia di notificazione di cartelle esattoriali che tengano conto della normativa sulla tutela dei dati personali, non sembra precludere l'emanazione di disposizioni ai sensi del cit. art. 1, comma 1, lett. *i*) della l. n. 676/1996, e conferma anzi la necessità e l'urgenza di interventi legislativi in materia.

2.1.8 «Riccometro» e «sanitometro»

La l. n. 449/1997, provvedimento legislativo «collegato» alla legge finanziaria per l'anno 1998, ha delegato il Governo a emanare appositi decreti legislativi al fine di:

a) definire criteri unificati per la valutazione della situazione economica dei cittadini che intendano beneficiare di prestazioni sociali agevolate in ambito pubblico, e di individuare le modalità per l'acquisizione delle informazioni necessarie per essere ammessi a tali prestazioni, nonché le relative forme di controllo (cd. «riccometro»: art. 59, comma 51);

b) riordinare il sistema di partecipazione al costo delle prestazioni sanitarie e del regime delle esenzioni (cd. «sanitometro»: art. 59, comma 50).

In attuazione di tale delega, la Presidenza del Consiglio dei ministri, oltre a sentire le competenti commissioni parlamentari, ha trasmesso gli schemi di decreti legislativi al Garante per acquisirne il parere.

Senza entrare nel merito delle scelte di politica economica e sociale, il Garante ha ritenuto che entrambi i decreti dovessero essere ampiamente perfezionati in modo da renderli conformi ai principi sanciti dalla l. n. 675/1996 e ai criteri di delega indicati dal Parlamento che rilevano nella materia dei dati personali.

Le osservazioni dell'Autorità, benché formulate in distinti momenti, hanno riguardato aspetti in larga parte comuni ai due schemi di decreto.

Il Garante, in via generale, ha lamentato la genericità della regolamentazione di cornice fornita dagli articolati rispetto ai trattamenti di dati personali connessi all'introduzione dei nuovi strumenti. La disciplina di tali trattamenti viene infatti demandata a successive fonti, alcune di carattere sicuramente regolamentare, altre non precisamente definite.

È stata fatta presente la necessità di superare la frammentazione di compiti e attribuzioni tra i vari enti interessati attraverso una regolamentazione comune e un'incisiva attività di coordinamento, nonché di garantire direttamente, con norme di rango primario, i diritti fondamentali degli interessati, soprattutto rispetto ai prospettati flussi di dati personali fra i soggetti erogatori delle prestazioni e altri soggetti pubblici.

Con particolare riferimento al trattamento di dati sensibili (specie sanitari) o comunque «delicati» (es. situazioni di convivenza), è stata rappresentata la necessità di eliminare la norma che prefigurava un consenso scritto dell'interessato, e di inserire nel testo legislativo una disposizione che indicasse invece le finalità perseguite, i dati utilizzabili e le operazioni eseguibili (v. anche § 2.1.4).

Riguardo alle modalità dei trattamenti effettuati dalle amministrazioni interessate (comuni, enti erogatori e centri di assistenza fiscale per il «riccometro», e aa.ss.ll. per il «sanitometro»), il Garante ha poi considerato necessario che fossero chiariti alcuni passaggi-chiave. Tali passaggi riguardano, in particolare:

- l'acquisizione delle dichiarazioni sostitutive e le informazioni in esse contenute per il rilascio dell'attestazione provvisoria valevole per l'ammissione alle agevolazioni;
- la registrazione dei dati in appositi archivi elettronici e la comunicazione ad altri soggetti;
- l'abilitazione a gestire le informazioni rilevate (anche con riferimento alle misure organizzative e tecniche per la protezione e la sicurezza dei dati).

L'Autorità ha suggerito di adottare specifici accorgimenti anche riguardo alla certificazione rilasciata al richiedente (nella quale sembrerebbe riportato l'intero contenuto della dichiarazione), per mascherare o rendere anonime alcune informazioni personali dell'interessato.

Hanno destato, infine, dubbi le disposizioni sui controlli diretti ad accertare la veridicità delle informazioni fornite da coloro che richiedono le esenzioni o le agevolazioni. Tali controlli, secondo lo schema originario del provvedimento relativo al «riccometro», avrebbero potuto essere effettuati anche in deroga alle leggi vigenti. Per la natura dei diritti coinvolti è emersa invece, ad avviso del Garante, la necessità di definire nel decreto legislativo quantomeno l'ambito e le modalità dei trattamenti correlati a queste procedure di controllo, nonché l'eventuale istituzione del servizio comune, e di individuare poi i requisiti minimi, in tema di informazioni personali, rispetto alle convenzioni da stipulare con il Ministero delle finanze.

Con particolare riferimento allo schema di decreto sul «sanitometro», è stata segnalata infine la totale carenza dello schema per ciò che riguarda le garanzie connesse all'introduzione della carta sanitaria, le quali devono essere previste anche nei confronti dell'eventuale prima fase di sperimentazione (v. anche § 2.6.4).

Anche per i tempi ristretti di approvazione, il Governo ha recepito, nei decreti legislativi nn. 109/1998 («riccometro») e 124/1998 («sanitometro»), solo alcune delle indicazioni fornite dal Garante, sottolineando comunque, in linea generale, il carattere sperimentale della disciplina dettata dai decreti stessi.

In entrambi i decreti legislativi è stata però eliminata la norma relativa al consenso degli interessati, anche se non è stata introdotta, come richiesto, una disposizione per precisare le finalità perseguite dal trattamento dei dati personali e le operazioni eseguibili.

Con specifico riferimento al decreto sul «riccometro», è stata poi individuata una specifica disposizione con la quale è stato precisato, in conformità a quanto indicato nella legge delega, che la Guardia di finanza potrà effettuare il controllo sostanziale della posizione reddituale e patrimoniale dei nuclei familiari dei soggetti beneficiari delle prestazioni agevolate secondo criteri selettivi stabiliti dalla direttiva annuale impartita dal Ministero delle finanze per le attività di accertamento (art. 4, comma 8, d.lg. 109/1998). Inoltre, sono state delineate specificamente alcune prestazioni escluse dal campo di applicazione dello stesso.

A seguito delle osservazioni del Garante sulla genericità delle norme in materia di trattamento dei dati, nel decreto legislativo sul «sanitometro» è stato introdotto un inciso in base al quale i regolamenti governativi da emanarsi ai sensi dell'art. 17, comma 2, della l. n. 400/1988 «dovranno determinare i criteri per lo svolgimento dei controlli sulle esenzioni riconosciute e per il trattamento dei dati personali con particolare riferimento alle modalità di utilizzazione dei dati, ai soggetti che possono accedervi e al tempo di conservazione dei dati stessi, nel rispetto delle disposizioni» sul trattamento dei dati (art. 6, comma 1, d.lg. n. 124/1998).

Questa previsione ha generato però qualche equivoco tanto che l'Autorità si è dovuta pronunciare successivamente, manifestando ampie perplessità, sullo stesso schema di decreto ministeriale recante il regolamento di individuazione delle malattie croniche e invalidanti da emanarsi secondo l'art. 5, comma 1, del d.lg. n. 124/1998.

In primo luogo, infatti, si è richiamata l'attenzione sulla necessità che le norme in materia di protezione dei dati personali vengano emanate, conformemente alla delega legislativa contenuta nell'art. 6 del citato d.lg. n. 124/1998, tramite regolamenti governativi di delegificazione (art. 17, comma 2, l. n. 400/1988) anziché attraverso regolamenti ministeriali (art. 17, comma 3, l. n. 400/1988).

È stato rilevato poi che la semplice sostituzione delle patologie invalidanti con codici di riferimento non presenta alcuna garanzia per l'anonimato degli interessati, data la facile associabilità delle une agli altri da parte dei numerosi soggetti che potrebbero accedere alla tabella di corrispondenza fra i codici e le patologie (e considerata la semplicità dei codici medesimi, facilmente memorizzabili da chiunque).

In sostanza, le integrazioni apportate nei due decreti legislativi hanno sanato solo in parte le perplessità sollevate dal Garante in materia di tutela dei dati personali.

Si segnala pertanto l'esigenza che il Governo predisponga, quanto prima, appositi emendamenti integrativi e aggiuntivi ai decreti già emanati. Tali disposizioni potrebbero essere adottate, in particolare, con uno dei decreti legislativi appositamente previsti dall'art. 6 del d.lg. n. 109/1998 (richiamato anche dall'art. 6, comma 3 del d.lg. n. 124/1998), il quale stabilisce che le informazioni personali acquisite possano essere utilizzate nel rispetto dei principi previsti dalla l. n. 675/1996 e delle disposizioni «che saranno dettate ai sensi del comma 1, anche al fine di assicurare la perdurante efficacia del sistema dei controlli».

2.1.9 Dichiarazioni dei redditi

Il tradizionale sistema di presentazione delle dichiarazioni dei redditi è stato innovato in occasione delle scadenze previste per il 1998.

L'art. 7 del d. lg. 9 luglio 1997, n. 241 ha modificato l'art. 12 del d.P.R. n. 600/1973, stabilendo che le dichiarazioni dei redditi non vadano più presentate o inviate direttamente all'Amministrazione finanziaria, ma siano inoltrate a essa, per via telematica, da banche o uffici postali convenzionati, ovvero tramite centri di assistenza fiscale, associazioni di categoria e professionisti (commercialisti, periti commerciali, consulenti del lavoro).

Il nuovo sistema così delineato, volto a velocizzare l'acquisizione dei dati da parte dell'Amministrazione finanziaria, ha creato però qualche problema in relazione alla legislazione sulla protezione dei dati personali. Nella maggior parte dei modelli, infatti, sono inseriti i riquadri per l'effettuazione delle scelte relative alla devoluzione dell'8 e del 4 per mille del gettito Irpef. Tali scelte evidenziano un dato sensibile, in quanto sono rispettivamente idonee a rivelare le convinzioni religiose o filosofiche degli interessati ovvero le loro idee politiche.

Per poter trattare tali dati, i soggetti intermediari hanno bisogno del consenso dell'interessato (che non è invece necessario per trattare i dati diversi da quelli sensibili, in quanto, essendo il loro conferimento obbligatorio per legge, si applica l'art. 12, comma 1, lett. a) della l. n. 675/1996). Malgrado alcuni approfondimenti in atto, i modelli inizialmente predisposti, però, non avevano tenuto conto di tale necessità.

Nell'imminenza della presentazione delle dichiarazioni dei redditi, il Governo ha quindi emanato il d.lg. n. 135/1998, il quale, all'art. 2, ha introdotto una nuova modifica al già citato d.P.R. n. 600/1973, aggiungendovi l'articolo *12-bis*.

Tale norma ha stabilito che con i decreti ministeriali di attuazione del nuovo sistema di presentazione delle dichiarazioni si sarebbero dovute prevedere anche le modalità per inserire nei modelli l'informativa all'interessato e l'espressione del consenso al trattamento dei dati sensibili. La stessa norma ha però previsto che in via transitoria, e limitatamente alle dichiarazioni presentate nel 1998, tale informativa doveva intendersi resa attraverso i modelli di dichiarazione e il consenso validamente espresso con la sottoscrizione delle dichiarazioni.

Questa soluzione normativa è stata oggetto di varie critiche anche in sede parlamentare. In particolare, esaminando un successivo schema di d. lg. sui dati sensibili nella Pa, poi approvato con il d. lg. n. 389/1998, la II commissione giustizia del Senato ha segnalato la necessità di evitare disposizioni di tal genere che rischiano di vanificare lo spirito e la lettera della legislazione sulla protezione dei dati personali.

Su un altro piano, la distribuzione dei modelli delle dichiarazioni dei redditi, e in particolare di quelli relativi a «Unico '98», ha sollevato diverse perplessità da parte dell'opinione pubblica con specifico riferimento al tipo di busta ideata per contenerli.

Quest'ultima, infatti, per consentire all'impiegato dell'ufficio postale o della banca di apporre direttamente sulla dichiarazione il timbro di ricezione, presentava un'ampia «finestra» dalla quale, secondo le segnalazioni di molti interessati, era possibile osservare alcuni dati inseriti nella dichiarazione e anche estrarre l'intero modello.

Alcune segnalazioni sono pervenute anche all'Ufficio del Garante e sono state esaminate nella riunione del 26 maggio 1998. Dalle verifiche effettuate si è constatata la possibilità, per chi riceveva la dichiarazione, di osservare i dati contenuti nel frontespizio e, in qualche misura, anche di estrarre il modulo.

Il riconoscimento della fondatezza dei reclami avrebbe reso necessaria, a rigore, secondo quanto affermato dalla stessa Autorità, l'immediata sostituzione della busta con un modello più idoneo; tuttavia ciò avrebbe reso inevitabile un sensibile differimento legislativo dei termini di presentazione della dichiarazione (sarebbe stato necessario, infatti modificare il decreto di approvazione del modello della busta e provvedere alla sua ristampa e distribuzione).

Il Garante ha quindi ritenuto che si potesse trovare una diversa soluzione che, senza arrecare gravi danni all'erario, garantisse comunque precise ed elevate misure di sicurezza e riservatezza dei dati dei contribuenti.

Tale soluzione è stata individuata negli schemi di convenzione fra Ministero delle finanze, banche ed Ente Poste, che erano in quel momento in corso di predisposizione. L'Autorità ha infatti precisato che tali schemi avrebbero dovuto prendere in attenta considerazione le finalità del trattamento effettuato dagli intermediari, imponendo un'attenta selezione del numero di persone aventi accesso ai dati relativi alle dichiarazioni e prevedendo la necessaria designazione degli addetti alla ricezione delle dichiarazioni quali «incaricati» del trattamento ai sensi degli artt. 8 e 19 della l. n. 675/1996.

Il Garante ha quindi verificato l'inserimento di tali prescrizioni, sia in sede di esame degli schemi convenzionali che gli sono stati sottoposti sia, soprattutto, al momento di rendere il proprio parere ai sensi dell'art. 31, comma 2 della l. n. 675/1996 sullo schema di decreto ministeriale di approvazione delle modalità tecniche di trasmissione telematica delle dichiarazioni.

In tale occasione l'Autorità ha suggerito precisi correttivi, registrando con soddisfazione il loro quasi integrale recepimento nel testo definitivo (decreto del Direttore generale del Dipartimento delle entrate del 31 luglio 1998).

In particolare, sono stati inseriti puntuali obblighi per gli intermediari in ordine all'individuazione dei soggetti destinati a trattare i dati personali contenuti nelle dichiarazioni dei redditi e alle misure da adottarsi per la loro ricezione e conservazione, garantendo all'Amministrazione finanziaria, anche con controlli a campione, il diritto di verificare il rispetto delle disposizioni in materia di protezione dei dati personali. La violazione di tali disposizioni è stata espressamente contemplata quale possibile caso di revoca dell'abilitazione del servizio.

La complessa vicenda connessa al trattamento dei dati relativi alle dichiarazioni si è così evoluta in modo positivo, prendendo spunto da una questione più specifica (la «finestra» sulla busta) e approdando poi a un sistema articolato di garanzie e di misure di sicurezza che ha certamente incrementato il grado di tutela degli interessati.

Nel secondo semestre del 1998 sono iniziati poi alcuni contatti informali fra l'Amministrazione finanziaria e l'Ufficio del Garante ai fini della predisposizione dei modelli di informativa da inserire nelle dichiarazioni dei redditi per l'anno 1999 e dell'individuazione delle modalità di prestazione del consenso al trattamento dei dati sensibili in esse contenuti, secondo quanto previsto dal ricordato art. 12-bis del d.P.R. n. 600/1973.

Per alcuni modelli di dichiarazione, il Ministero delle finanze ha quindi formalizzato la richiesta di parere a questa Autorità (con ritardo, però, rispetto alla già avvenuta pubblicazione di alcuni di essi) il 30 dicembre 1998 (v. § 3.1.3).

L'informativa da rendere agli interessati è stata inserita nelle istruzioni per la compilazione dei modelli ed è stato precisato che la firma apposta in uno dei riquadri relativi alla scelta del 4 e dell'8 per mille ha valore anche come prestazione del consenso al trattamento. Tale soluzione ha permesso di evitare una serie di problemi

connessi all'eventualità che, anche solo per distrazione, alla firma apposta in calce alla scelta effettuata non seguisse la firma per il consenso o viceversa. L'avvertenza è stata riprodotta più volte a maggior garanzia del contribuente.

Per le dichiarazioni da presentarsi a banche e uffici postali è stata confermata, da parte dell'Amministrazione finanziaria, la scelta di utilizzare buste con finestra, le cui dimensioni sarebbero state tuttavia ridotte al minimo indispensabile in modo da rendere impossibile l'estrazione delle dichiarazioni senza creare evidenti lacerazioni degli involucri. È stato eliminato poi dal primo foglio della dichiarazione ogni dato personale diverso da quelli anagrafici visibili dalla finestra, e lo spazio restante è stato riempito dall'informativa sulla protezione dei dati personali.

Il Garante ha preso atto dei modelli di informativa predisposti e di quanto dichiarato dal Ministero delle finanze riguardo alle informazioni ivi inserite circa il flusso dei dati, alle modalità e alle logiche utilizzate. Analogamente, non avendo ricevuto alcun esemplare da verificare, l'Autorità ha preso atto dell'assicurazione che le dimensioni ridotte della busta siano tali da impedirne l'estrazione del contenuto.

Successivamente sono stati sottoposti al Garante, per il prescritto parere, gli schemi relativi ad altri modelli di dichiarazioni.

2.1.10 Appalti

Tra le materie che a seguito dell'entrata in vigore della l. n. 675/1996 sono state oggetto di numerosi quesiti al Garante rientra anche quella degli appalti pubblici.

Alcune amministrazioni hanno chiesto di conoscere se per verificare la capacità tecnica e/o finanziaria dei concorrenti sia lecito chiedere informazioni relative non solo a tali soggetti, ma anche a terzi che in precedenti circostanze siano stati destinatari di simili forniture o servizi prestati dal medesimo partecipante alla gara.

Quesiti analoghi sono stati posti, inoltre, da alcune imprese in ordine alla necessità di acquisire il consenso dei clienti ai quali si riferiscono le informazioni da fornire alle amministrazioni appaltanti.

A tale proposito il Garante ha osservato che non si rinvenivano ostacoli di principio al trattamento di tali dati. Anche in questa fattispecie, infatti, è applicabile il principio secondo cui i soggetti pubblici - a differenza dei privati e degli enti pubblici economici - non devono richiedere il consenso degli interessati per poter trattare dati riferiti a persone fisiche o giuridiche, ma devono piuttosto verificare che i singoli trattamenti siano riconducibili alle proprie finalità istituzionali e siano posti in essere rispettando le specifiche limitazioni eventualmente previste dalle norme speciali di riferimento (art. 27, comma 1, l. n. 675/1996).

La normativa vigente in materia di appalti pubblici di beni e servizi prevede che le amministrazioni possano richiedere ai concorrenti di dimostrare le proprie capacità tecniche fornendo l'elenco dei principali servizi o forniture prestati negli ultimi tre anni, con l'indicazione degli importi, delle date e dei destinatari (art. 14, d.lg n. 157/1995 e art. 14, d.lg. 358/1992).

Il Garante ha evidenziato che le imprese partecipanti, laddove (come avviene nella prevalenza dei casi) si tratti di dati relativi allo svolgimento di attività economiche, possono comunicare alle amministrazioni i dati relativi ai terzi già destinatari di simili forniture, senza che sia necessario richiedere il consenso degli interessati (artt. 12, comma 1, lett. *f*) e 20, comma 1, lett. *e*) della l. n. 675/1996). Resta però ferma l'esigenza del rispetto della vigente normativa in materia di segreto aziendale e industriale.

Resta parimenti ferma la necessità di modellare comunque le informative che le imprese forniscono ai rispettivi clienti ai sensi dell'art. 10 della l. n. 675/1996, tenendo conto, appunto, dell'eventualità che alcuni dati siano forniti, a richiesta, ad amministrazioni appaltanti.

Il Garante ha sottolineato, inoltre, la necessità che le amministrazioni rispettino le vigenti disposizioni a tutela della riservatezza o degli altri diritti delle società partecipanti alle gare, disposizioni previste nell'ordinamento anche al di fuori della l. n. 675/1996 ovvero nell'ambito della disciplina sugli appalti. Tali disposizioni prescrivono, tra l'altro, di chiedere le sole informazioni non eccedenti l'oggetto, tenendo in debito conto «gli interessi legittimi del concorrente relativi alla protezione di interessi tecnici e commerciali» (art. 14, comma 3, d.lg. 157/1995, e in termini quasi identici, art. 14, comma 3, d.lg. 358/1992).

Da ultimo è da segnalare che alcuni quesiti pervenuti in materia di appalti pubblici sono comunque ricollegabili all'accesso agli atti della pubblica amministrazione, per cui valgono le considerazioni già formulate al riguardo (v. § 2.1.3).

2.2 INFORMATIVA ALL'INTERESSATO E CONSENSO

2.2.1 Complessità dei vecchi moduli e semplificazioni

L'informativa e il consenso costituiscono due aspetti fondamentali della nuova disciplina prevista dalla direttiva 95/46/CE e dalla l. n. 675/1996 per il trattamento dei dati personali, essendo espressione diretta dei principi di correttezza e di liceità nella raccolta e nell'utilizzazione delle informazioni.

Tali adempimenti, che per il settore pubblico riguardano soltanto l'informativa, sono anche quelli che hanno coinvolto maggiormente, e in modo più immediato, gli operatori di ogni settore, poiché incidono nelle attività quotidiane (professionali, commerciali o istituzionali) e nei normali rapporti che intercorrono, in particolare, con gli utenti, i clienti e i dipendenti.

Nella fase di prima applicazione della legge sono emersi diversi problemi in ordine alla corretta esecuzione degli obblighi in materia di informativa e di richiesta del consenso agli interessati. Nel primo anno di attività il Garante è intervenuto più volte per garantire il pieno rispetto delle disposizioni vigenti, fornendo anche alcuni criteri generali in modo da rendere più semplici e comprensibili gli appositi modelli predisposti, ad esempio, da banche, da compagnie di assicurazione e da altre società (v., in particolare, la *Relazione per l'anno 1997*, cap. 4.4, pag. 72 e ss.).

Nel 1998 è continuata questa attività di collaborazione per assicurare sostanziali e adeguate garanzie a tutela dei diritti degli interessati e, allo stesso tempo, di chiarimento degli adempimenti connessi alla raccolta e al trattamento delle informazioni personali, anche sulla base di una campagna di informazione dei cittadini e di impulso attraverso comunicati stampa, gruppi di lavoro, seminari e conferenze, assistenza telefonica, ecc., affinché le imprese adottino forme semplificate di informazione degli interessati.

Gli inconvenienti e le difficoltà che sia le organizzazioni imprenditoriali, sia i cittadini hanno incontrato nell'attuazione di questi adempimenti sono quelli che hanno accompagnato nei vari Paesi la fase d'avvio della disciplina sulla protezione dei dati personali. Questa disciplina introduce, infatti, un sistema avanzato di tutela delle persone, che richiede però una partecipazione attiva e un grado maggiore di consapevolezza da parte dei soggetti interessati.

Era pertanto del tutto fisiologico che, in questa prima fase, le cospicue novità introdotte dalla l. n. 675/1996 determinassero un certo disagio che ha portato anche alcuni cittadini a considerare come un fastidio quello che costituisce, invece, uno strumento assai utile in chiave di trasparenza e di tutela dei diritti della propria personalità.

Si deve tuttavia rilevare che, al di là del fenomeno fisiologico, gli stessi operatori che gestiscono dati personali, limitandosi ad adottare modelli di informativa che non fornivano reali chiarimenti sulle modalità e sulle finalità del trattamento, hanno alimentato vari dubbi negli interessati, inducendoli talvolta in errore e, comunque, non ponendoli in condizione di fornire una pronta manifestazione del consenso.

Nel 1998 questa Autorità ha svolto un'attività di verifica sul pieno rispetto dei principi già affermati in precedenti provvedimenti, soprattutto per quanto riguarda il *settore creditizio e finanziario*, sulla base sia di un'apposita indagine conoscitiva svolta richiedendo informazioni e modelli a numerosi istituti di credito, sia dell'attivazione di specifici gruppi consultivi con le principali istituzioni e società bancarie.

In sintesi si è appurato che, a seguito delle indicazioni generali fornite dal Garante, i cui contenuti sono stati ampiamente riportati sulla stampa, varie società operanti specie nel settore bancario hanno riformulato i modelli già distribuiti ai propri clienti, inviandoli nuovamente alla clientela.

La nuova modulistica distribuita dalle banche, per quanto ancora complessa e non facilmente comprensibile per il cittadino, è apparsa in linea generale conforme ai principi evidenziati dal Garante, prevedendo essa, di regola, la possibilità per la clientela di esprimere un distinto consenso «informato» nei riguardi dei trattamenti non strettamente connessi ai servizi richiesti contrattualmente (in riferimento, ad esempio, all'invio di materiale pubblicitario e, in genere, all'offerta di prodotti e servizi anche di società terze), senza che ciò abbia riflessi sul contratto medesimo.

Tuttavia, molti clienti non hanno ancora fornito un riscontro ai modelli inviati dalle banche e dalle altre società operanti nel settore e si è creato, pertanto, il problema della mancanza del consenso. Problema che è stato in parte superato con la soluzione del tutto temporanea già prospettata dal Garante, per cui, nell'attesa del rilascio della dichiarazione relativa al consenso, la richiesta di una prestazione da parte del cliente (es.: l'emissione di un assegno) è stata considerata come una manifestazione di volontà equiparabile al consenso per le operazioni di trattamento connesse a quella prestazione, sia pure in via del tutto provvisoria.

Pertanto, vi è la necessità che la clientela rimasta inerte sia nuovamente stimolata a esprimere il proprio consenso. Il Garante ha preso atto di alcune iniziative in corso nel settore bancario volte a richiamare l'attenzione della clientela con messaggi inviati, ad esempio, a margine degli estratti conto.

Al tempo stesso, il Garante ha avviato una autonoma riflessione e si è impegnato a suggerire schemi di modelli che, pur mantenendo ferme le sostanziali garanzie a tutela dei diritti degli interessati, siano più semplici e meglio comprensibili, in modo da permettere ai clienti di fornire più agevolmente un rapido riscontro alle richieste di consenso formulate dalle società bancarie (v. al riguardo, cap. 2.10).

Una prima bozza di informativa semplificata è stata sottoposta nel febbraio del 1999 alla attenzione del pubblico e degli operatori del settore anche attraverso la sua pubblicazione su alcuni quotidiani. Sono pervenute alcune proposte e osservazioni che il Garante ha considerato in tempi brevi suggerendo, così, uno schema di informativa standard.

2.2.2 Chiarezza delle informative ed esoneri

Come è noto, l'informativa rappresenta una delle condizioni per la validità del consenso e consiste nell'indicazione, alla persona cui si riferiscono i dati, degli elementi principali del loro trattamento da parte di colui che li raccoglie (finalità e logiche perseguite, ambito di divulgazione dei dati all'esterno, possibilità dell'esercizio di specifici diritti di accesso, ecc.).

Secondo l'orientamento ribadito da questa Autorità nel corso del 1998 in relazione a diversi settori, l'informativa:

- può essere fornita agli interessati, oralmente o per iscritto, *una tantum* da ogni soggetto, pubblico e privato, che acquisisca e gestisca dati personali, dovendo essere rinnovata solo quando cambi una delle informazioni essenziali previste dall'art. 10 della l. n. 675/1996;

- deve essere distinta sul piano concettuale, anche se può essere fornita contestualmente per entrambi i casi, a seconda che la raccolta dei dati avvenga presso la persona cui questi si riferiscono, oppure presso terzi (in tale ultima ipotesi l'informativa va comunicata all'interessato al momento della registrazione dei dati o della loro prima comunicazione ai terzi - art. 10, comma 3);

- può anche essere in parte orale e in parte scritta, o fornita attraverso l'affissione del documento in spazi utilizzati per una efficace informazione al pubblico.

In particolare, il Garante ha segnalato alle pubbliche amministrazioni (ministeri, regioni, comuni, università e altri organismi) che appaiono ancora in notevole ritardo rispetto a tale adempimento, la necessità di dare attuazione agli obblighi di informativa nella raccolta dei dati personali, suggerendo peraltro modalità semplificate di informazione ai cittadini soprattutto quando il trattamento sia effettuato in base a obblighi di legge o di regolamento (ad esempio, attraverso modelli esplicativi in forma sintetica, da consegnare direttamente agli interessati ed eventualmente da affiggere anche negli uffici o presso gli appositi sportelli adibiti ai rapporti con il pubblico).

Tuttavia sono state riscontrate ancora diverse carenze in tema di informativa, in ambito sia pubblico sia privato. Fra le più ricorrenti si segnalano la mancanza di chiarezza sulla natura obbligatoria o facoltativa del conferimento dei dati, l'insufficiente delimitazione dell'ambito di comunicazione e di diffusione e l'assenza di spiegazioni in ordine ai principali criteri e metodologie di elaborazione.

Più in generale, questa Autorità ha rilevato che i primi modelli distribuiti da soggetti operanti nei vari campi sono risultati spesso del tutto «tautologici» e generici, essendosi determinata una preferenza per formulazioni troppo ampie e al tempo stesso complesse, che hanno sortito l'effetto di confondere o, peggio, di insospettire l'interessato, al punto di ostacolare una manifestazione di volontà, quale che essa fosse. Dovrebbero ora essere realizzate informative semplici nel linguaggio e nel contenuto, specifiche e da collegare in modo più immediato al servizio o alla prestazione richiesta dal cittadino (utente-cliente). Di qui anche l'impegno dell'Autorità a formulare schemi esemplificativi per agevolare la corretta esecuzione di questo obbligo, su cui si riferirà meglio nell'ultima parte del presente paragrafo.

Specie a seguito della recente emanazione del regolamento governativo sull'organizzazione e il funzionamento del Garante (d.P.R. 31 marzo 1998, n. 501, in G.U. n. 25 del 1° febbraio 1999), sarà peraltro necessario, per i casi di sostanziale violazione dell'obbligo di informativa, provvedere all'applicazione delle sanzioni amministrative pecuniarie di cui all'art. 39 della l. n. 675/1996.

Nel corso dei primi due anni di applicazione della legge sono pervenute inoltre numerose istanze con le quali diversi soggetti hanno chiesto di essere esonerati dall'obbligo di fornire l'informativa agli interessati, così come previsto dall'art. 10, comma 4, in caso di raccolta di dati presso terzi. Larga parte di queste richieste - riguardanti i dati raccolti dai clienti, dai fornitori, dai dipendenti, ecc. ai fini della tenuta della contabilità e dell'adempimento di obblighi fiscali e retributivi, i trattamenti svolti nel settore pubblico, i *curricula vitae* inviati spontaneamente alle aziende o i dati degli abbonati a quotidiani e periodici - non sono state accolte, in quanto formulate in modo del tutto generico o prive di adeguata motivazione, oppure sono state giudicate inammissibili, perché non soddisfacevano i parametri individuati dall'art. 10, comma 4, della l. n. 675/1996 o erano riconducibili a ipotesi di trattamento per le quali la legge stessa non obbliga a informare gli interessati.

Al riguardo, l'Autorità ha ritenuto però necessario fornire alcune indicazioni di carattere generale in modo da chiarire l'esatto ambito applicativo delle disposizioni sull'informativa. In sintesi il Garante ha ricordato che:

- l'informativa relativa ai dati raccolti presso terzi non deve essere fornita quando i dati siano utilizzati per adempiere a obblighi normativi o per lo svolgimento di investigazioni difensive penali, ovvero per la difesa di un diritto in sede giudiziaria;

- la richiesta di esonero dall'informativa può trovare accoglimento da parte del Garante, in via eccezionale (nel caso in cui l'informativa stessa comporti un impiego di mezzi manifestamente sproporzionati o si riveli impossibile: v. citato art. 10, comma 4), relativamente, sempre, ai soli dati raccolti presso terzi;

- a sostegno delle richieste di esonero devono essere addotte comprovate motivazioni e concreti elementi di riscontro, con particolare riferimento alla speciale natura delle finalità perseguite o dei dati trattati, alle complesse modalità di realizzazione dell'adempimento, all'ingente numero degli interessati, alle attività necessarie per rintracciarli, alla data di raccolta delle informazioni o alla particolare onerosità dei costi da sostenere.

A tale proposito l'Autorità ha altresì prospettato, ai fini dell'eventuale riconoscimento dell'esonero, la possibilità di valutare, in circostanze particolari, modalità di informazione sostitutive di quelle rivolte caso per caso a ciascun interessato (per es., mediante avvisi pubblici o annunci periodici, specie sulla stampa nazionale o locale anche specializzata).

Una informativa analoga è stata ad esempio inserita nel *codice di deontologia* recentemente adottato dai giornalisti in tema di tutela dei dati personali. Accanto alle ridotte e, in alcuni casi, non obbligatorie informazioni che il singolo giornalista deve fornire all'interessato al momento della raccolta dei dati (rendendo note la propria identità, la propria professione e le finalità perseguite: v. l'art. 2 del codice), è infatti prevista una forma di informativa «pubblica» o «impersonale» per i dati personali comunque utilizzati presso le testate giornalistiche e le imprese editrici, le quali devono rendere nota al pubblico mediante annunci, almeno due volte l'anno, l'esistenza dei propri archivi (v. § 2.3.2 e 2.3.3).

2.2.3 Libertà e specificità del consenso

In relazione alla gestione del consenso, questa Autorità ha ribadito alcuni principi della l. n. 675/1996 applicabili a tutti i soggetti privati, chiarendo che:

- sono del tutto inammissibili le pressioni su clienti e interessati per conseguire un loro consenso generale;

– la formula di consenso, preceduta da una chiara e corretta informativa, deve essere precisa e ben articolata, con la previsione di specifiche opzioni per l'interessato; queste devono essere di tipo «positivo», dovendo permettere di esprimere o di negare il consenso;

– il consenso deve essere manifestato in forma scritta solo se si tratta di dati sensibili, mentre negli altri casi è sufficiente che esso, se necessario, sia espresso «in forma specifica e documentata per iscritto» (v. art. 11, comma 3, l. n. 675/1996); ad esempio, nell'ipotesi di collegamento telefonico, attraverso la documentazione da parte dell'operatore che raccoglie le informazioni.

In diversi provvedimenti, l'Autorità ha fornito inoltre chiarimenti per ciò che attiene ai casi di esclusione del consenso, con particolare riferimento all'adempimento di obblighi normativi e ai dati riguardanti lo svolgimento di attività economiche da parte dell'interessato. Il Garante ha ritenuto che in quest'ultima espressione rientrino anche gli aspetti economici dell'attività svolta da imprenditori individuali o da liberi professionisti, ma ha escluso che la stessa espressione possa essere interpretata fino al punto di ricomprendervi ogni informazione personale a sfondo economico, anche quando, ad esempio, il dato riguardi attività puramente personali o familiari di una persona.

Questo approccio è stato da ultimo ribadito in un parere reso all'Autorità garante della concorrenza e del mercato il 16 febbraio 1999, ove si è ricordato che:

a) la predetta interpretazione risulta indirettamente confermata dalla lettura delle disposizioni di precedenti testi legislativi relativi ad altre materie, nei quali l'espressione «attività economiche» viene utilizzata con specifico riferimento ad attività produttive, industriali, commerciali o comunque concernenti la produzione di beni o di servizi, anche nel terziario, da considerarsi in modo del tutto distinto rispetto ad altri aspetti e attività delle persone;

b) una interpretazione dell'espressione «dati relativi allo svolgimento di attività economiche» fuori della *ratio legis* porterebbe a uno svuotamento della disciplina in materia di dati personali o ad un significativo aggiramento di molte sue disposizioni. Un riferimento al dato economico *tout court* finirebbe, tra l'altro, per avvalorare la tesi erronea secondo cui qualsiasi informazione utilizzata dal titolare nello svolgimento della propria attività economica può essere ricondotta nella menzionata esigenza del consenso.

È stata altresì ulteriormente precisata la differente disciplina in tema di consenso tra i soggetti privati e quelli pubblici, i quali ultimi non operano, come si è detto, in base al consenso degli interessati, bensì secondo le proprie funzioni istituzionali e le norme di riferimento (v. § 2.1.1 e 2.1.4).

Parimenti rilevanti sul predetto tema (e su quello dell'informativa) sono apparse le indicazioni fornite da questa Autorità in materia di dati sensibili e sanitari, in riferimento a strutture sanitarie, medici, enti previdenziali e assistenziali, ecc. (v. capp. 2.6 e 2.7), nonché i chiarimenti concernenti il settore del lavoro e, da ultimo, l'attuazione dei menzionati adempimenti nel mercato del lavoro temporaneo e interinale.

Infine, un problema rilevante in ambito finanziario, come in quello assicurativo, si è posto per quanto riguarda l'espressione del consenso nei confronti del «circuito» o della «catena» di ulteriori soggetti che possono venire a conoscenza dei dati e svolgere determinati trattamenti puramente strumentali e temporanei rispetto a quello dell'originario titolare. Al riguardo, stante l'opportunità di evitare l'eccessivo moltiplicarsi di informative e di consensi, andrebbe ricercata una soluzione che permetta a un titolare del trattamento, all'inizio del rapporto con l'interessato, di acquisire *una tantum* il consenso anche per conto di alcuni altri titolari di trattamenti strettamente connessi e funzionali ai servizi e alle prestazioni richieste dagli interessati,

mediante un'indicazione precisa delle relative categorie e il rinvio a un elenco puntuale costantemente aggiornato e prontamente accessibile con facilità dal pubblico, ad esempio mediante un sito *Web*, un numero verde o una missiva inviata immediatamente a domicilio. Soggetti che, d'altra parte, devono restare distinti da quelli che svolgono stabilmente autonomi trattamenti dei dati, per i quali deve essere invece rilasciato un separato e puntuale consenso.

Nonostante sussistano simili possibilità di semplificazione, alcune associazioni di categoria di vari settori economici e produttivi ritengono che tali adempimenti siano comunque ancora gravosi e avanzano ad esempio l'ipotesi di una integrazione, in sede di decretazione delegata, dell'art. 20 della l. n. 675/1996, per avvicinarlo alle previsioni degli artt. 12 e 28 sull'esclusione del consenso per i trattamenti dei dati connessi all'esecuzione degli obblighi contrattuali.

Ove il Governo ritenga di esercitare la delega a tale proposito, andrà in ogni caso rispettata l'impostazione di fondo prescelta dal Parlamento, che ha portato a ritenere tuttora necessaria una specifica consapevolezza del contraente in ordine alla divulgazione dei suoi dati all'esterno, e che potrebbe, ad esempio, condurre a legittimare la comunicazione dei dati nei casi in cui questa sia oggetto di una precisa previsione contrattuale sottoposta alla specifica e realmente consapevole accettazione dell'interessato (sempre in quest'ultimo caso, la comunicazione dei dati presupporrebbe una particolare consapevolezza dell'interessato che potrebbe non sfociare in una distinta manifestazione del consenso).

2.3 GIORNALISMO E INFORMAZIONE

2.3.1 Lo sviluppo della l. n. 675/1996 in riferimento all'attività giornalistica

L'anno appena trascorso è stato denso di eventi rilevanti in tema di giornalismo e attività di informazione. È un settore, questo, nel quale il trattamento dei dati personali pone da sempre in modo particolarmente evidente problemi di bilanciamento tra tutela della persona e libertà di stampa e di manifestazione del pensiero: comprensibile, quindi, che l'introduzione della l. n. 675/1996, con tutto il carico di novità che essa recava in attuazione della direttiva europea n. 95/46/CE, comportasse un impatto complesso e impegnativo e, insieme, richiedesse tempi e modi per verificarne i primi effetti e apportare gli opportuni aggiustamenti.

Il legislatore, dal canto suo, aveva mostrato sensibilità al riguardo. Infatti, oltre ad aver enucleato una speciale disciplina per alcuni aspetti originale, in tema di trattamento dei dati effettuato nell'esercizio della professione di giornalista, aveva messo a disposizione, con la l. n. 676/1996, lo strumento del decreto delegato per emanare norme integrative e correttive, lasciando a una fonte duttile, quale un apposito codice deontologico dei giornalisti relativo al trattamento dei dati personali, la specifica regolazione di ulteriori e non secondari profili a tutela della persona.

E in effetti questi meccanismi di adeguamento e di affinamento, accortamente previsti, hanno avuto uno sviluppo concreto.

Già nell'anno di avvio della legge - anche a seguito del ruolo attivo svolto dal Garante, in collaborazione con il Governo, per assicurare il massimo rispetto dell'art. 21 della Costituzione - era stata esercitata la delega per alcuni primi opportuni interventi.

In particolare, la disciplina prevista per i giornalisti veniva estesa ai trattamenti effettuati dai pubblicitari e dai praticanti, nonché da coloro che trattano temporaneamente dati finalizzati alla pubblicazione o alla diffusione occasionale di articoli,

saggi e altre manifestazioni del pensiero (art. 25, comma 4-bis, della l. n. 675/1996, aggiunto dal d.lg. 9 maggio 1997, n. 123). Poi, si introduceva la possibilità di una notificazione in forma semplificata per i giornalisti, i pubblicisti e i praticanti e si disponeva l'esonero dall'obbligo di notificazione per i predetti autori di articoli, saggi e simili (art. 7, rispettivamente commi 5-bis, lett. b), e 5-ter, lett. n), della l. n. 675/1996, aggiunti dal d.lg. 28 luglio 1997, n. 255). Si consentivano, quindi, a favore dei giornalisti e degli altri soggetti operanti nel settore, forme semplificate per le informative di cui all'art. 10 della legge, rinviando al Codice deontologico la loro concreta individuazione (art. 25, comma 4, della l. n. 675/1996, come integrato dal d.lg. 9 maggio 1997, n. 123).

A questi decreti ha fatto seguito una seconda fase di elaborazione normativa, che è stata occasione per ulteriori interventi volti a chiarire, precisare e adeguare meglio la disciplina rispetto alla specifica natura dell'attività giornalistica. Anche in questa circostanza la partecipazione attiva del Garante ha svolto un ruolo non secondario, di segnalazione, di proposta, di cooperazione, nel delicato dialogo con il Governo, per favorire il raggiungimento di soluzioni equilibrate. Ruolo analogo, del resto, è stato svolto nel rapporto con l'Ordine dei giornalisti, anche perché, quasi parallelamente, veniva condotto l'intenso lavoro di elaborazione del Codice deontologico, come si vedrà (§ 2.3.2).

Così, si è giunti all'emanazione del d.lg. 13 maggio 1998, n. 171 (della cui deliberazione da parte del Consiglio dei ministri, in data 9 aprile, si era potuto dare notizia anticipata nella *Relazione per l'anno 1997*), sul quale il Garante ha espresso anche formalmente parere favorevole.

Il decreto è tornato su due temi cruciali che ancora mostravano di richiedere soluzioni e precisazioni adeguate: il trattamento dei dati personali, soprattutto di tipo cd. «particolare», e il Codice deontologico.

La disciplina relativa al trattamento dei dati particolari (cioè i dati sensibili e quelli relativi a determinati provvedimenti di carattere giudiziario, di cui rispettivamente agli artt. 22 e 24 della l. n. 675/1996) effettuato nell'esercizio della professione giornalistica (art. 25) è apparsa subito molto controversa e in grado di suscitare dubbi interpretativi.

Pertanto è stata abbandonata l'originaria formulazione, secondo cui il giornalista, mentre poteva prescindere dal consenso dell'interessato quando trattava dati «comuni» e alcune categorie di dati sensibili (quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico politico o sindacale), doveva invece ottenere il consenso nel trattare gli altri dati sensibili, idonei a rivelare lo stato di salute e la vita sessuale; formulazione che inoltre, e soprattutto, era tale da non escludere chiaramente, per il trattamento dei dati sensibili di ogni tipo, la previa autorizzazione da parte del Garante (comunque esclusa subito, in via interpretativa, dall'Autorità stessa, nel pieno rispetto dell'art. 21 Cost.).

Si è, all'opposto, preferito riformulare il comma 1 dell'art. 25, in modo da eliminare ogni graduazione di disciplina tra dati sensibili e rendere immediatamente esplicito che autorizzazione e consenso (nonché i limiti per il trattamento dei dati personali relativi a provvedimenti giudiziari, di cui all'art. 24) non si applicano quando il trattamento dei dati «particolari», di ogni tipo, è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità.

È risultato peraltro opportuno precisare che resta salva la possibilità di trattare i dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico, confermando peraltro (e facendone oggetto di statuizione autonoma) il dovere di rispettare i limiti del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione riguardo a fatti d'interesse pubblico.

Dopo una fase di confronto aperto, vivo e talora polemico, che ha visto impegnato il mondo dell'informazione, queste soluzioni hanno incontrato vasto consenso, come dimostrano anche le posizioni assunte dall'Ordine dei giornalisti.

Consenso raggiunto, attraverso un'analogia evoluzione del dibattito, anche intorno al secondo importante tema affrontato dal decreto, quello del Codice di deontologia relativo al trattamento dei dati personali.

Qui la scelta operata sin dall'inizio dal legislatore - recependo l'esplicita indicazione fornita dagli artt. 9 e 27 della direttiva comunitaria 95/46/CE - non ha dato adito a perplessità e si è rivelata, anzi, quanto mai opportuna e corretta: l'affidare la definizione di regole in tema di diritto all'informazione e di libertà di manifestazione del pensiero proprio alla responsabilità di alcuni dei soggetti portatori di questi diritti fondamentali (in cooperazione con l'Autorità di garanzia) è, infatti, il segno di una convinta adesione ai principi posti dall'art. 21 della Costituzione.

La delega, dunque, è stata utilizzata per inserire alcune integrazioni puntuali ma importanti, volte a precisare sia il ruolo del Garante al riguardo, sia l'ambito di intervento del Codice e la sua natura.

Infatti l'orientamento ad arricchire il contenuto del Codice e a rafforzarne la posizione nel sistema delle fonti del diritto si è sviluppato parallelamente all'altro, teso ad alleggerire la disciplina legislativa nella parte concernente il trattamento dei dati personali effettuato dai giornalisti.

Ad esempio, nel riservare al Codice la determinazione di misure e accorgimenti a garanzia degli interessati rapportate alla natura dei dati, si prescrive una particolare attenzione per quanto riguarda quei dati idonei a rivelare lo stato di salute e la vita sessuale, recuperando così, in parte e con modalità diverse, quella specifica protezione che questa categoria di dati aveva perso a seguito della modifica dell'art. 25, comma 1, della l. n. 675/1996, di cui si è detto.

Quanto al Garante, poi, si dispone che cooperi con il Consiglio dell'ordine nella fase di formazione del Codice e successivamente, e si stabilisce che abbia la competenza a curare la pubblicazione del Codice nella «Gazzetta Ufficiale», come si vedrà qui di seguito.

2.3.2 Il Codice deontologico

Il «Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica», di cui all'art. 25 della l. n. 675/1996, contiene le regole di condotta da rispettarsi in materia e contribuisce, in funzione delle specificità del settore, alla corretta applicazione della legislazione sulla riservatezza.

È lo strumento che l'ordinamento ha previsto per contemperare i diritti fondamentali della persona con il diritto dei cittadini all'informazione e con la libertà di stampa, ritenendo preferibile rispondere alle nuove esigenze di regolazione attraverso il ricorso a regole integrative e specifiche del dettato legislativo in una prospettiva nuova rispetto alle forme tradizionali di autoregolamentazione (talvolta rivelatesi inefficaci sul piano dell'effettività delle prescrizioni).

Una originalità, questa, che ha portato a qualificare il Codice stesso non come un tradizionale codice deontologico, ma come una fonte secondaria, sia pure atipica, dell'ordinamento.

In un primo momento, tuttavia, il ruolo e la portata effettivi del Codice non sono stati percepiti appieno e si è dato luogo ad accese polemiche, soprattutto in alcuni ambienti giornalistici, sin dal momento in cui, il 26 maggio 1997, il Garante ha invitato il Consiglio nazionale dell'ordine dei giornalisti ad avviare la redazione del Codice e ad adottarlo. La fase di elaborazione, accompagnata da un ampio dibattito, si è protratta per tutta la prima metà del 1998 ed è stata comunque occasione per una rinnovata consapevolezza da parte del sistema politico e della società civile intorno a un tema delicato e di viva attualità.

La prima bozza del Codice è stata predisposta in sostanziale coincidenza con il termine semestrale previsto dalla legge. Il suo perfezionamento e la sua definitiva adozione da parte del Consiglio nazionale dell'Ordine hanno però richiesto vari incontri e approfondimenti. Il procedimento di adozione del Codice si è poi intersecato con la modifica dell'art. 25 della legge, auspicata dal Garante nel gennaio del 1998 e operata nel mese di aprile con il citato d.lg. 171/1998, il che ha comportato l'inevitabile differimento della formalizzazione del codice stesso, che altrimenti sarebbe stato superato subito dal medesimo decreto legislativo.

L'Autorità, poiché, come è noto, non ha soltanto il potere di avviare questo processo, ma, in base alla legge, può svolgere una funzione di impulso e di controllo durante tutto l'arco della formulazione del Codice (e anche successivamente, per verificarne l'attuazione), ha inteso porsi come punto di riferimento costante nel corso dei lavori e, anche nei momenti di più serrato confronto, ha sempre curato di mantenere aperti canali di dialogo con l'Ordine, con la categoria dei giornalisti e con la stessa opinione pubblica, in modo da realizzare un proficuo scambio di idee e suggerimenti a chiarimento delle rispettive posizioni e a beneficio di una migliore predisposizione del testo.

Alcune osservazioni toccavano aspetti di fondo. Si sollecitava, ad esempio, il pieno rispetto dei punti contenuti nella «Carta di Treviso», sottoscritta dai giornalisti il 4-5 ottobre 1990 per sottoporre a rigorose cautele l'utilizzazione delle notizie relative ai minori. Oppure si criticava una prima impostazione del testo, che sembrava limitarsi a porre mere norme deontologiche interne, la cui violazione sarebbe stata sanzionabile solo sul piano disciplinare, mentre la novità, da valorizzare, era proprio il «codice» inteso come sostanziale fonte del diritto, di rango secondario, che entra a far parte dell'ordinamento giuridico generale e deve essere rispettata da tutti coloro che esercitano attività d'informazione attraverso mezzi di comunicazione. Questo carattere di generalità tipico della fonte trova oggi conferma nella prevista pubblicazione del Codice nella «Gazzetta Ufficiale».

Per quanto attiene invece agli aspetti più strettamente formali del procedimento di formazione dell'atto, è da sottolineare l'importante ruolo affidato al Consiglio nazionale dell'Ordine dei giornalisti, al quale spetta adottare il Codice in cooperazione con il Garante; e naturalmente, vanno richiamate le peculiari competenze del Garante, tra cui spiccano un potere di iniziativa, per promuovere l'adozione; un potere di forte impulso e stimolo sui contenuti, per prescrivere eventuali misure e accorgimenti a garanzia degli interessati; un potere di verifica di legittimità e di riscontro della rispondenza e dell'idoneità delle misure; un potere sostitutivo eventuale; un potere di disporre l'opportuna pubblicazione espressamente prevista dal d.lg. n. 171/1998 (artt. 25, commi 2 e 3, e 31, comma 1, lett. h)).

La pubblicazione è stata disposta dal Garante il 29 luglio 1998, ed è avvenuta pochi giorni dopo (G.U. 3 agosto 1998, n. 179).

Con riferimento ai contenuti, poi, il testo del Codice esordisce con alcune enunciazioni di principio, per ricordare che, in forza dell'art. 21 Cost., la professione giornalistica si svolge senza autorizzazioni o censure e che, in quanto condizione essen-

ziale per l'esercizio del diritto-dovere di cronaca, la raccolta e la diffusione di notizie nell'ambito dell'attività giornalistica si differenziano dalla memorizzazione e dal trattamento di dati personali a opera di banche dati o altri soggetti; su tali principi si fondano le deroghe alla normativa comunitaria (art. 9 direttiva n. 95/46/CE) e a quella nazionale.

Quindi individua le forme semplificate di informativa, distinguendo tra quelle spettanti al giornalista e quelle facenti capo all'editore; precisa che il giornalista, nel raccogliere notizie, evita artifici e pressioni indebite; richiama l'attenzione sugli archivi personali e le banche dati redazionali (art. 2 del Codice). Rafforza l'obbligo di rettificare senza ritardo errori o inesattezze (art. 4). Conferma il diritto all'informazione in presenza di dati sensibili, nel rispetto però dell'essenzialità dell'informazione, in modo da evitare riferimenti ad altri soggetti non interessati ai fatti (art. 5), e della sfera privata delle persone note o che esercitano funzioni pubbliche, se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica (art. 6). Detta norme specifiche a tutela della riservatezza e della personalità del minore, valori da considerare sempre primari rispetto al diritto di critica e di cronaca, e accoglie i principi e i limiti stabiliti dalla «Carta di Treviso» (art. 7). Fornisce poi criteri per assicurare la tutela della dignità delle persone (art. 8). Con riferimento ai «dati particolari», pone infine precetti a tutela del diritto alla non discriminazione (art. 9), nonché della dignità, della riservatezza e del decoro delle persone malate (art. 10) e della sfera sessuale della persona (art. 11), e, ancora, in materia di cronaca nei procedimenti penali (art. 12).

Il testo completo del Codice è riportato negli Allegati.

2.3.3 Prime applicazioni della nuova normativa

La casistica che il Garante è stato chiamato a esaminare è molto diversificata e tocca rilevanti aspetti dell'attività giornalistica:

a) Un primo quesito posto dal comitato di redazione di un noto quotidiano era volto a ottenere chiarimenti in tema di *notificazione* dei trattamenti di dati da parte dei giornalisti.

Nella risposta (del 24 marzo 1998), il Garante ha inteso dissipare dubbi in ordine all'interpretazione della legge al riguardo e, in via generale, ha richiamato l'ipotesi particolare nella quale le informazioni sono raccolte e utilizzate in una dimensione strettamente privata da parte di chiunque, giornalisti compresi, a uso personale o professionale, e l'ha distinta dall'altra in cui, invece, le informazioni sono destinate «ad una comunicazione sistematica o alla diffusione» (art. 3 della l. n. 675/1996). Solo in quest'ultima ipotesi, infatti, si applica la legge e vanno rispettati tutti gli adempimenti da essa previsti per la protezione dei dati personali, tra cui l'obbligo di notificazione (art. 7, in attuazione della direttiva europea n. 95/46/CE del 24 ottobre 1995).

La notificazione, comunque, riguarda non i singoli dati contenuti nell'archivio, ma, semplicemente, l'esistenza di un archivio contenente dati personali (come definiti dall'art. 1, comma 2, lett. c) della legge) e le caratteristiche generali del loro trattamento (definito dall'art. 1, comma 2, lett. b)). E per i giornalisti, a ulteriore e specifica garanzia, viene salvaguardata la riservatezza delle fonti della notizia e «restano ferme le norme sul segreto professionale» (art. 13, comma 5). Poi, per uno specifico intervento del legislatore, il settore dell'informazione può giovare dello snellimento di alcuni adempimenti: la notifica in forma *semplificata*, per i giornalisti, i pubbli-

cisti, i praticanti (art. 7, comma 5-ter, lett. b)), e l'esonero da essa per coloro che trattano dati temporaneamente ai fini della pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero (art. 7, comma 5-ter, lett. n)).

Pertanto, alcuni timori manifestati anche vivacemente dalla stampa, in un primo momento, circa la portata della nuova legge e i rischi di limitazione della libertà di informazione sono apparsi ben presto eccessivi.

Restava da chiarire chi fosse il soggetto tenuto alla notificazione semplificata. Come è noto, questi è il *titolare* del trattamento, cioè il soggetto cui competono le decisioni di fondo sulle finalità e sulle modalità del trattamento (art. 1, comma 2, lett. d)).

Con riferimento all'ambito specifico dell'impresa giornalistico-editoriale, il Garante ha ritenuto corretto e aderente alla realtà identificare tale figura con l'*editore*, anziché, necessariamente, con i singoli giornalisti collaboratori. A tale conclusione si è giunti attraverso un'analisi del modo di esplicazione dell'attività giornalistica e del rapporto giornalisti-editori, oggetto di riflessioni analoghe anche in altri Paesi. Elementi rilevanti in tal senso sono stati previsti anche dal contratto di lavoro giornalistico, soprattutto nella parte in cui riconosce un ruolo decisivo dell'editore nell'organizzare e programmare l'utilizzazione dei sistemi elettronici editoriali e di ogni altro supporto tecnologico da parte delle redazioni, e nelle altre parti in cui disciplina il rapporto tra editore e singoli giornalisti per ciò che riguarda l'utilizzazione e le modalità di formazione degli archivi redazionali.

Peraltro, la notificazione riguarda l'insieme delle banche dati automatizzate e cartacee utilizzate a scopi giornalistici, anche quando (come accade normalmente) le informazioni sono frammentate in più archivi, computer o fascicoli posti in uno o più luoghi nella materiale disponibilità dei singoli giornalisti, sono poi riversate solo in parte in una banca dati comune e, quindi, possono non essere condivise da alcuni collaboratori. Anche in questi casi, *una* è la notificazione, attraverso un unico atto, in quanto la dichiarazione generale non si riferisce a singoli archivi, computer, schedari, ma attiene al complesso dell'attività di raccolta, elaborazione e diffusione delle informazioni; è dovuta «una sola volta», «a prescindere dal numero delle operazioni da svolgere, nonché dalla durata del trattamento» (art. 7, comma 2); e, potendo riguardare «più trattamenti con finalità correlate» tra loro, può riassumere contestualmente sia i trattamenti di dati destinati direttamente alle finalità giornalistiche, sia quelli che l'impresa gestisce a fini amministrativi o commerciali.

Tale soluzione ha avuto effetti di semplificazione dell'attività dei singoli, in vari contesti: nelle imprese che pubblicano quotidiani e periodici, nelle case editrici che curano libri, collane e altre pubblicazioni, nelle ipotesi in cui il giornalista operi senza un vincolo di subordinazione o collabori contemporaneamente a più quotidiani ed è l'impresa, o le imprese, a effettuare la notificazione.

Diverso e residuale è il caso del giornalista che non si limiti a tenere materiale informativo «per fini esclusivamente personali», ma crei una distinta base di dati «destinati ad una comunicazione sistematica o alla diffusione» (art. 3, comma 1), operando in una condizione di completa autonomia dall'editore e al di fuori di quelle particolari modalità di lavoro previste dal contratto collettivo con riferimento alla struttura editoriale: in tal caso, infatti, egli assume la veste di titolare del trattamento e deve effettuare una notificazione al Garante, anche in questa ipotesi *una tantum*.

b) In altra occasione è stato richiesto un intervento del Garante in tema di modalità di raccolta dei dati personali, con particolare riferimento al principio di correttezza affermato dall'art. 9 della l. n. 675/1996.

Veniva segnalato un episodio verificatosi a seguito di un'intervista rilasciata da un parlamentare a un telegiornale: all'insaputa dell'interessato, alcuni brani erano stati registrati "fuori onda" e trasmessi poi nel corso di un programma televisivo a sfondo satirico.

L'Autorità si è pronunciata (il 22 luglio 1998) osservando preliminarmente che, nel caso in esame, erano in questione non il diritto di informare il pubblico sulle opinioni che i rappresentanti politici esprimono anche attraverso dichiarazioni non ufficiali, né la configurabilità della satira televisiva tra le attività giornalistiche, bensì i profili della correttezza nel trattamento e dell'indicazione esplicita dello scopo della raccolta (art. 9, comma 1, lett. *a*) e *b*)). Occorreva considerare che la legge, e le sue successive modificazioni e integrazioni (cui presto si sarebbe aggiunto il Codice deontologico, allora non ancora pubblicato), per quanto abbiano introdotto una normativa largamente distinta proprio per tener conto delle esigenze specifiche del mondo dell'informazione (come la possibilità di raccogliere e divulgare dati e notizie personali anche senza il consenso degli interessati), non prevedono e non giustificano alcuna deroga alla disciplina contenuta nell'art. 9.

Pertanto, i dati e le informazioni, contenuti anche su supporti audiovisivi, devono essere raccolti – dal giornalista, al pari di ogni altro soggetto – «secondo correttezza», senza violenza o inganno e per scopi determinati ed espliciti. Il dovere di "lealtà" nei confronti del soggetto cui si riferiscono le notizie opera sin dal momento della loro raccolta, caratterizza l'intera attività di trattamento e impegna anche al momento della loro divulgazione all'esterno (trovando ad esempio traduzione, all'interno del Codice dei giornalisti, nell'obbligo di informativa, seppure semplificata, e nel dovere di evitare «artifici e pressioni indebite»).

Su questo piano, la convinzione dell'interessato, che risultava evidente nel caso in esame, di non essere oggetto di una registrazione in quel determinato momento meritava considerazione da parte dei responsabili della trasmissione. Il principio di correttezza certamente è leso laddove emergano elementi oggettivi che rivelino un intento di inganno o di preordinazione, volto a indurre gli intervistati a dialogare o ad esprimere opinioni nel convincimento dell'assenza di una registrazione; ma il principio va rispettato anche nel caso di registrazioni accidentali o che non facciano parte di una prova di trasmissione. E comunque, ove sia concretamente impossibile al momento della registrazione, la correttezza va rispettata nel prosieguo e in particolare nel caso in cui si intenda procedere alla diffusione.

Dunque i responsabili della trasmissione avrebbero dovuto astenersi dal diffondere la registrazione, malgrado lo sfondo satirico nel quale essa veniva inserita, e quantomeno avrebbero dovuto darne tempestiva notizia all'interessato ponendolo in grado di esprimere tempestivamente il proprio punto di vista ed, eventualmente, di opporsi all'ulteriore trattamento. Il Garante, pertanto, ha segnalato alla rete televisiva la necessità di tener conto dei principi e di rendere conformi a essi i trattamenti, ai sensi dell'art. 31, comma 1, lett. *c*) della legge.

c) Alcuni quesiti pervenuti all'Autorità concernevano l'interpretazione di talune parti del Codice di deontologia relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica: ad esempio la disposizione secondo cui, «se i dati sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a rendere noti al pubblico, mediante annunci, almeno due volte l'anno, l'esistenza dell'archivio e il luogo dove è possibile esercitare i diritti previsti dalla legge n. 675/1996» (art. 2, comma 2, del Codice cit.).

Alla richiesta se ciò renda superfluo adempiere all'obbligo di informativa agli interessati previsto dalla legge (art. 10), il Garante ha risposto (l'11 agosto 1998) che l'*informativa*, pur nell'unitarietà del suo fondamento e delle sue finalità, va data

seguendo non una modalità unica, ma modi diversi secondo le due distinte situazioni in cui possono essere raccolti i dati: direttamente presso l'interessato, o indirettamente presso terzi (art. 10, rispettivamente commi 1 e 3). E ha sottolineato come le forme semplificate che, anche riguardo a questo tema, il legislatore ha inteso consentire a favore dell'attività giornalistica, lasciando poi che venissero specificate dal Codice deontologico, corrispondono a queste distinte ipotesi di raccolta dei dati (art. 25, comma 4, della l. n. 675/1996, come integrato dal d.lg. 9 maggio 1997, n. 123).

Ora, la semplificazione che si traduce nella possibilità di una informativa generale da parte dell'*editore*, mediante *annunci*, copre esclusivamente la seconda ipotesi, in cui il giornalista raccolga le informazioni presso terzi ovvero attinga alle varie fonti informative disponibili.

Resta ferma, invece, perché non v'è ragione di ritenerla sostituibile o superflua, l'informativa che il *giornalista* è in grado di dare *direttamente* all'interessato, dal vivo, al momento stesso in cui raccoglie i dati. E questa continua a essere un dovere del giornalista, oltre che a rispondere a un'esigenza di correttezza. Qui il legislatore, da parte sua, aveva già iniziato tempestivamente a semplificare la disciplina originaria, consentendo di informare anche oralmente, oltre che per iscritto, con immediato beneficio per il lavoro dei cronisti (art. 10, comma 1, della l. n. 675/1996, come integrato dal d.lg. n. 123/1997). La semplificazione introdotta, a sua volta, dal Codice consiste nella possibilità di un'informativa assai più snella nei contenuti, limitata al rendere palese il fatto che si sta esercitando un'attività giornalistica e al rendere note la propria identità, la professione, le finalità della raccolta - a meno che ciò risulti impossibile o comporti rischi per l'incolumità del professionista - senza poi dover specificare necessariamente gli altri elementi richiesti in via generale dall'art. 10 della legge (art. 2, comma 1, del Codice cit.). Dunque, questa informativa spetta al giornalista; l'altra, all'editore (o, anche questa, al giornalista che operi in situazioni di completa autonomia, come sopra evidenziato).

Alla richiesta di chiarimenti circa le modalità per provvedere ai predetti *annunci*, il Garante ha poi sottolineato (l'11 agosto 1998, nella medesima occasione) che il Codice prevede due distinti adempimenti.

Da un lato, indicare (accanto ai tradizionali dati obbligatori per legge quali, ad esempio, il nome del direttore responsabile) il nominativo e la sede della persona fisica o giuridica che svolge le funzioni di responsabile del trattamento dei dati, precisando che presso tale figura possono essere esercitati in concreto i diritti dell'interessato previsti dalla l. n. 675/1996 (come quelli di accesso, rettifica, aggiornamento, integrazione dei dati, ecc.).

Dall'altro, ove l'impresa editoriale gestisca banche dati di uso redazionale, rendere nota la loro esistenza al pubblico, almeno due volte l'anno, con un annuncio sulla propria testata ed eventualmente su altre.

È stato sollevato poi il problema del diritto di *accesso* ai dati personali. Quanto alla possibilità che l'interessato faccia valere i propri diritti presso il titolare o il responsabile del trattamento, il Garante ha posto in evidenza come questo meccanismo di tutela basato su un rapporto diretto sia stato voluto dal legislatore (all'art. 13) per favorire la risoluzione non contenziosa e rapida dei conflitti in materia. Ove però questa via si riveli infruttuosa, la stessa l. n. 675/1996 prevede che le parti possano rivolgersi all'autorità giudiziaria, secondo le ordinarie procedure, oppure al Garante, attraverso ricorsi ai sensi dell'art. 29 (fatta salva la possibilità di inviare comunque a quest'ultimo segnalazioni e reclami).

Sul punto specifico concernente il comportamento da tenere da parte del titolare o responsabile del trattamento di fronte a una richiesta di cancellazione dei dati, il Garante ha fatto presente che deve essere compiuta una verifica in concreto per appurare se la richiesta sia fondata e da accogliere integralmente (ad esempio, se il dato è stato raccolto illecitamente), o se possa essere soddisfatta intervenendo sul trattamento senza procedere, però, alla cancellazione totale, ove, per renderlo conforme alla legge, sia sufficiente l'aggiornamento, l'integrazione, la rettifica dei dati (se erronei o inesatti, in base all'art. 4 del Codice cit.) o l'eliminazione di alcune notizie (se non essenziali per il diritto di cronaca).

d) In altra occasione il quesito rivolto all'Autorità mirava a conoscere se fosse esercitabile nei confronti dell'editore di un quotidiano e di una giornalista collaboratrice il diritto di «accesso» ai dati personali previsto dall'art. 13, per ottenere la registrazione di una intervista rilasciata dall'interessato al quotidiano stesso e divenuta poi oggetto di un articolo.

Il Garante ha risposto (il 26 novembre 1998) ricordando che i diritti di accesso sono riconosciuti nei confronti di entrambe le figure, le quali devono confermare senza ritardo se detengono o no dati personali che riguardano l'interessato e devono comunicarli all'interessato stesso in una forma intellegibile (come già affermato con il provvedimento del 16 ottobre 1997, in Bollettino n. 2, pag. 72). La clausola di salvaguardia del segreto professionale, se può essere opposta all'interessato che chieda la fonte della notizia (cfr. art. 13, comma 5, della l. n. 675/1996 e art. 2, comma 3, della l. n. 69/1993), evidentemente non opera quando, come nel caso in esame, la fonte è l'interessato stesso che ha rilasciato l'intervista al giornalista. Il Codice di deontologia fornisce un sostegno in tal senso (v., in particolare, art. 2, commi 2 e 3).

Si è quindi ritenuto che il diniego a fornire la registrazione non trovasse adeguata motivazione nella dichiarazione con la quale il giornalista aveva dichiarato di non disporre di un archivio inquadrabile nell'ambito della legge sulla *privacy*. Infatti la l. n. 675/1996 riguarda le operazioni di trattamento dei dati personali (ad esempio, la raccolta, l'utilizzazione, l'elaborazione e la divulgazione) a prescindere dal fatto che le informazioni trattate siano contenute in una banca-dati, in un archivio o altro.

Né il diniego trovava idonea motivazione nell'argomentazione secondo cui la registrazione dell'intervista non sarebbe da ritenersi un dato personale, accessibile ai sensi dell'art. 13. La legge, infatti, in armonia con gli atti internazionali e comunitari che ha attuato, considera come «dato personale» qualunque informazione che consenta l'identificazione dei soggetti interessati, anche se derivante da suoni o da immagini (come appunto una registrazione sonora, una foto, un filmato); in ogni caso, un'intervista, un colloquio, come qualsiasi altra dichiarazione, opinione o manifestazione del pensiero proveniente dall'interessato, costituiscono senz'altro informazioni che riguardano la sua persona e, come tali, dati personali, senza che sia rilevante la forma in cui essi sono trattati o gli eventuali supporti che li contengano.

Di conseguenza, il Garante si è pronunciato nel senso di riconoscere all'interessato un diritto pieno di ottenere la comunicazione dei propri dati personali da parte dell'editore o, direttamente, del giornalista, in una forma chiaramente intellegibile (ad esempio, una riproduzione su supporto sonoro o cartaceo), come prevede la legge (art. 13, comma 1, lett. c), n. 1).

Anche di fronte all'eventuale esigenza per il giornalista di difendersi in sede giudiziaria, l'esercizio dei diritti da parte dell'interessato non incontra limiti se non reca pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto alla difesa (art. 14, comma 1, lett. e)).

e) Il Garante ha ricevuto poi un reclamo contro alcuni organi di stampa che avevano pubblicato senza consenso articoli e notizie riguardanti un minore coinvolto in un incidente, rivelandone le esatte generalità e alcuni dati particolari, e che, nonostante l'espressa richiesta avanzata dai genitori dell'interessato, non avevano assunto l'impegno a non effettuare in futuro ulteriori trattamenti.

L'Autorità (in data 8 settembre 1998) ha ritenuto fondato il reclamo, poiché la pubblicazione dei dati personali del minore risultava essere non essenziale rispetto al fatto di interesse pubblico verificatosi e certamente non essenziale ai fini dell'esercizio del diritto di cronaca. Inoltre, il trattamento di quei dati sarebbe dovuto avvenire con particolare attenzione considerata anche la posizione di tutela che l'ordinamento riserva ai minori e l'esplicita previsione dell'art. 13, comma 1, del d.P.R. n. 448/1988 che vieta la pubblicazione e la divulgazione di notizie idonee a consentire l'identificazione del minorenne comunque coinvolto nel procedimento penale. Principi che sono stati affermati in passato nella «Carta di Treviso» e che sono ora sanciti nel Codice di deontologia.

Di conseguenza, il Garante ha vietato l'ulteriore trattamento dei dati personali idonei a identificare il minore interessato, ai sensi dell'art. 9, comma 1, lett. a) e d), dell'art. 20, comma 1, lett. d) e dell'art. 31, comma 1, lett. l) della l. n. 675/1996.

f) In relazione a un grave fatto di cronaca, il Garante è stato chiamato a pronunciarsi in merito alla diffusione, da parte di un quotidiano nazionale, dei dati di una persona che in passato aveva convissuto con la vittima del delitto.

L'Autorità (il 12 ottobre 1998) ha ritenuto, da un lato, che la diffusione dell'indirizzo dell'interessato realizzasse un'interferenza nella sfera privata non giustificata ai fini dell'esercizio del diritto di cronaca, perché non essenziale rispetto al fatto di interesse pubblico; pertanto, ha disposto il divieto di ulteriore diffusione di tali dati (ai sensi degli artt. 9, comma 1, lett. a) e 20, comma 1, lett. d) e dell'art. 31, comma 1, lett. l) della l. n. 675/1996).

Ha ritenuto, dall'altro, che il trattamento dei dati relativi al nome, all'immagine e alla professione dell'interessato potesse ritenersi giustificato solo quando la loro conoscenza fosse essenziale in ragione dell'eventuale ulteriore sviluppo dei fatti e del loro accertamento giudiziario; ha segnalato quindi all'editore e al direttore responsabile del quotidiano la necessità di conformare a questi principi il successivo trattamento dei dati (ai sensi dell'art. 31, comma 1, lett. c) della legge).

g) Il Garante ha inoltre ricevuto una segnalazione relativa alla pubblicazione della notizia di una sentenza di condanna penale su un quotidiano locale, episodio che veniva denunciato come lesivo della riservatezza e della onorabilità dell'interessato, il quale ricopriva la carica di consigliere comunale.

L'Autorità ha ritenuto (il 21 ottobre 1998) che il fatto non costituisca una violazione delle norme a tutela della riservatezza in quanto la diffusione della notizia della sentenza di condanna non viola le norme del codice relative al divieto di pubblicazione degli atti del processo penale (art. 114 c.p.p.) né altre specifiche norme; che è inoltre legittima la diffusione di dati personali nell'ambito dell'attività giornalistica, qualora essa avvenga nel rispetto dei limiti del diritto di cronaca e del criterio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

h) Da ultimo, si può far cenno a due recentissime decisioni che, pur nella diversità degli episodi segnalati, hanno riguardato entrambe alcuni nodi critici del rapporto tra il diritto di cronaca e i diritti della personalità.

Nel primo caso, in relazione al noto episodio avvenuto presso Gravina di Puglia, veniva richiesto l'intervento del Garante al fine di impedire il prosieguo della diffusione in ambito giornalistico di notizie di carattere strettamente privato concernenti la vittima.

L'Autorità (con provvedimento 8 marzo 1999) ha preso in attenta considerazione l'ampio risalto dato alla vicenda da parte della stampa e della televisione e ha posto in evidenza soprattutto due punti: da un lato, che il fatto era di interesse pubblico, ma che alcuni articoli si erano spinti oltre i limiti a tutela della riservatezza (diffusione di dati sanitari, vicende intime, atti e corrispondenze di natura personale, convinzioni religiose e abitudini personali della vittima e di altri, con scarsa attenzione per i diritti degli interessati), rivelando notizie o dettagli coperti da segreto professionale, d'ufficio o investigativo, oppure non essenziali per la necessaria informazione dell'opinione pubblica; dall'altro, che la dignità e i diritti della personalità devono essere rispettati nel trattamento dei dati personali anche nei confronti delle persone decedute, i cui diritti possono essere fatti valere da chiunque vi abbia interesse (art. 13, comma 3, della l. n. 675/1996).

Anche il codice di deontologia che, insieme alla l. n. 675/1996 e alle altre norme vigenti in materia, costituisce la normativa di riferimento per i giornalisti fa specifico richiamo al rispetto della dignità degli interessati (art. 8 del Codice), al principio di essenzialità dell'informazione, specie quando i dati divulgati siano di natura «sensibile» (artt. 5 e 6) e al dovere di omettere riferimenti a congiunti o ad altri soggetti non interessati ai fatti ovvero a dettagli di violenza (artt. 5 e 8).

Queste considerazioni hanno pertanto portato il Garante ad adottare un provvedimento (ai sensi dell'art. 31, comma 1, lett. c) della l. n. 675/1996) per invitare gli organi pubblici competenti a verificare se la diffusione dei dati sanitari sia avvenuta in violazione del segreto professionale o di quello d'ufficio o di indagine, e per segnalare ai mezzi di informazione la necessità di adeguare la raccolta e la diffusione dei dati alla normativa vigente, di cui il Codice di deontologia è parte integrante.

Un primo formale seguito dell'invito è stato dato dal Consiglio dell'Ordine dei giornalisti della Puglia che, in data 18 marzo 1999, ha sollecitato vari mezzi di informazione a fornire precisi elementi relativi ai servizi televisivi o radiofonici trasmessi, per valutare eventuali violazioni delle norme deontologiche della professione giornalistica.

i) In un contesto del tutto diverso, il Garante non ha ravvisato violazione della normativa, e ha ritenuto perciò la segnalazione non fondata, in un caso per il quale veniva lamentata la ripresa e la diffusione televisiva di immagini filmate riguardanti un personaggio noto del mondo dello spettacolo e ritenute lesive della sua *privacy*. Al termine dell'istruttoria, l'Autorità ha ritenuto (il 10 marzo 1999) che il ritrarre una persona nota, in luogo aperto al pubblico tale da rendere agevoli le riprese senza artifici o tecniche invasive, non incorra in alcuno dei limiti e delle prescrizioni che potrebbero essere richiamati al riguardo.

Il consenso dell'interessato non è infatti richiesto quando il trattamento e, in particolare, la diffusione dei dati siano effettuati «nell'esercizio della professione di giornalista»; l'episodio segnalato, inoltre, rientrava nell'ambito del diritto di cronaca, non essendo stati superati i limiti posti «a tutela della riservatezza ed in particolare dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico» (cfr. art. 12, comma 1, lett. e), art. 20, comma 1, lett. d) e art. 25 della l. n. 675/1996 e la disciplina integrativa recata dal Codice deontologico).

Del resto una normativa ben più risalente stabilisce che «non occorre il consenso della persona ritratta quando la riproduzione dell'immagine è giustificata dalla notorietà» (art. 97 della l. 22 aprile 1941, n. 633, sulla protezione del diritto d'autore).

2.4 ASSOCIAZIONI E PARTITI POLITICI

Il crescente fenomeno dell'associazionismo e il suo ruolo determinante assunto nel Paese nella gestione di numerosi servizi sociali comporta inevitabilmente il trattamento di una mole di dati personali riguardanti sia i singoli associati, sia i terzi con i quali tali organismi vengono in contatto per lo svolgimento delle attività statutarie.

Proseguendo nell'intento di semplificazione degli adempimenti previsti dalla l. n. 675/1996 a carico degli organismi associativi, il Garante ha rinnovato fino al 30 settembre 1999, senza mutamenti sostanziali rispetto alla precedente autorizzazione generale del 1997, l'esonero dall'obbligo di richiedere singolarmente l'autorizzazione per il trattamento dei dati sensibili relativi agli iscritti e ai sostenitori (autorizzazione n. 3/1998, in G.U. del 1° ottobre 1998, n. 229).

Peraltro, una novità introdotta dal nuovo provvedimento generale ha portato a estendere l'applicabilità della suddetta autorizzazione agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose, consentendo così il trattamento dei dati sensibili attinenti anche agli studenti iscritti o che hanno presentato domanda di iscrizione a detti istituti. È stato altresì consentito di trattare i dati sensibili dei lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali (v. anche cap. 2.8).

Per quanto attiene ai quesiti, sono stati forniti alcuni chiarimenti a un partito politico (provv. 8 gennaio 1998, in Bollettino, n. 3, p. 22) in merito al fatto che l'iscrizione al partito costituisce di per sé un dato sensibile per il cui trattamento è necessario che venga espresso il consenso scritto da parte dell'interessato, preceduto da un'idonea informativa allo stesso. A tal fine è stata suggerita una formula da riportarsi sul modulo di adesione che era stata peraltro pubblicizzata già dal Garante il 16 ottobre 1997.

A un altro partito politico (provv. 30 marzo 1998, in Bollettino, n. 4, p. 12) è stato precisato poi che non deve essere richiesta un'apposita autorizzazione per poter trattare i dati sensibili, essendo sufficiente osservare le disposizioni contenute nelle autorizzazioni generali nn. 1 e 3, riguardanti, rispettivamente, i rapporti di lavoro e gli organismi associativi. Con la medesima risposta il Garante ha altresì sottolineato che non è necessario notificare i trattamenti dei dati relativi ai dipendenti, ai simpatizzanti e agli aderenti, sempre che i dati siano utilizzati in conformità alle disposizioni dell'art. 7, comma 5-ter della l. n. 675/1996.

In relazione a un quesito formulato da un gruppo parlamentare in merito alla diffusione di opuscoli di propaganda politica ed elettorale contenenti dati definiti dalla legge come «sensibili», il Garante ha precisato (provv. del 30 marzo 1998, in Bollettino, n. 4, p. 28) che occorre valutare preliminarmente le caratteristiche

dell'opuscolo. Infatti, se quest'ultimo è curato da giornalisti o da pubblicisti per il perseguimento di finalità informative, benché nell'ambito di un'attività politica, non si deve chiedere il consenso dell'interessato (art. 25, comma 4-bis, della l. n. 675/1996).

Il Garante ha ritenuto tuttavia necessario sottolineare che, anche in tale contesto normativo, rimane immutata l'esigenza del rispetto di alcuni limiti posti al diritto di cronaca a tutela della riservatezza, integrati da talune regole contenute nel codice di deontologia (prov. 29 luglio 1998, G.U. n. 179 del 3 agosto 1998), specie per quanto riguarda l'essenzialità delle informazioni divulgate rispetto a fatti di interesse pubblico (artt. 12, comma 1, lett. e), 20, comma 9, lett. d) e 25). Nella medesima risposta il Garante ha affrontato anche il tema del trattamento dei dati di carattere giudiziario, ricordando che per tali dati è in vigore una norma transitoria che ne permette il trattamento fino all'8 maggio 1999, data entro la quale è prevista l'emanazione di norme integrative che dovranno prevedere alcune ulteriori garanzie.

Il Garante si è quindi espresso (prov. del 27 marzo 1998, in *Bollettino*, n. 4, p. 30) in riferimento alla tenuta di un indirizzario dei soci di un'associazione professionale a carattere culturale e sindacale, finalizzato alla trasmissione di un periodico mensile mediante abbonamento postale. Sull'argomento, l'Autorità ha esaminato due diverse ipotesi:

a) nel caso in cui il periodico sia spedito soltanto agli iscritti all'associazione, si è rilevato, la tenuta dell'indirizzario contenente i dati degli abbonati configura un trattamento di dati sensibili, in quanto «idonei a rivelare l'adesione a un'associazione sindacale». Ciò comporta che tali dati possano essere trattati solo dopo aver acquisito il consenso scritto dell'interessato e sulla base dell'autorizzazione del Garante. L'Autorità ha fatto peraltro presente che detto consenso scritto, previa informativa all'interessato in base all'art. 10, può essere acquisito in un'unica soluzione al momento in cui l'associazione medesima deve raccogliere l'adesione dei propri iscritti;

b) nella seconda ipotesi (in cui il periodico è spedito agli abbonati, a prescindere dalla loro iscrizione all'associazione), in cui sembravano venire in considerazione dati personali «comuni», il Garante ha precisato che, oltre all'informativa, salvo che si tratti di dati conoscibili da chiunque, è necessaria l'acquisizione del consenso dell'interessato, il quale può essere anche orale ma deve risultare, in ogni caso, da un documento scritto.

In relazione ad alcuni quesiti provenienti da un'associazione circa presunte schedature di persone omosessuali effettuate dalle forze dell'ordine, il Garante (prov. del 22 aprile 1998, in *Bollettino*, n. 4, p. 11), acquisiti elementi di valutazione dai Ministri dell'interno e della difesa (che hanno assicurato di non detenere elenchi di omosessuali e di non effettuare forme di schedatura o discriminazioni illegittime basate sulle abitudini o preferenze sessuali dei cittadini), ha comunicato all'associazione stessa l'esito degli accertamenti svolti, riservandosi di esercitare i propri poteri di controllo qualora pervengano ulteriori e circostanziate segnalazioni.

Rispondendo a un'associazione di analisti finanziari (prov. del 26 ottobre 1998, in *Bollettino*, n. 6, in corso di pubblicazione), il Garante ha infine evidenziato che anche per la stampa di un annuario soci da inviare agli associati e agli abbonati alla rivista dell'associazione, oltre all'informativa, occorre acquisire il consenso dell'interessato, salvo che si tratti di dati conoscibili da chiunque.

L'Autorità ha però precisato che il consenso, acquisibile anche all'atto della compilazione del formulario di richiesta di adesione all'associazione stessa, può essere documentato con una formula puntuale ma concisa, collegandolo alle attività previste dallo statuto (ove la pubblicazione dell'annuario e il suo invio agli abbonati siano previsti dallo statuto) o, più direttamente, alla stampa e diffusione dell'annuario stesso.

2.5 CONFESSIONI RELIGIOSE

In materia di confessioni religiose, nel 1998 va registrata l'attuazione di alcune importanti novità di carattere generale, anche di rango legislativo, e di vari interventi di tipo particolare.

Già nel corso del 1997, il d.lg. n. 255/1997 aveva introdotto alcune semplificazioni, modificando l'art. 7 della l. n. 675/1996 e includendo fra gli esoneri dall'obbligo di notificazione i trattamenti effettuati da associazioni, fondazioni e comitati aventi carattere filosofico e religioso (come pure quelli posti in essere da organismi rappresentativi di tali soggetti istituiti per scopi non di lucro, nonché da organizzazioni di volontariato).

Introducendo questo esonero il legislatore aveva opportunamente precisato che rimangono fermi gli obblighi di informativa agli interessati e di acquisizione del loro consenso, ove necessario. Accanto a tali obblighi, la disciplina introdotta dalla legge per il trattamento di dati sensibili, quali appunto quelli relativi all'adesione a una confessione religiosa, prevede anche l'autorizzazione del Garante.

Sempre nel 1997, al fine di semplificare anche quest'ultimo adempimento, il Garante aveva incluso tra le autorizzazioni generali rilasciate per diverse tipologie di titolari o di trattamenti, una autorizzazione (la n. 3/1997), che faceva riferimento al trattamento dei dati sensibili da parte degli organismi associativi, ivi comprese le confessioni religiose e le comunità religiose.

Nel corso del 1998 tale autorizzazione si è dimostrata efficace nel suo intento di combinare la semplificazione degli adempimenti con il rispetto di alcune garanzie. Al momento del suo rinnovo (30 settembre 1998) si è perciò reso necessario integrarla in due sole occasioni, con analoghe prescrizioni a carattere particolare che si è ritenuto opportuno demandare ad apposite autorizzazioni: nei confronti, cioè, di una società cattolica di assicurazioni e di un istituto scolastico privato (v. § 3.1.4).

Nel primo caso il trattamento di dati sensibili per il quale si chiedeva l'autorizzazione consisteva nella gestione dei dati relativi ai soci. Questi ultimi, infatti, secondo le previsioni statutarie della società, devono essere esclusivamente persone che professano la religione cattolica e che manifestano sentimenti di adesione alle opere cattoliche.

Nel secondo caso, invece, la richiesta di autorizzazione si legittimava con la necessità per l'istituto scolastico, che aveva forma di s.r.l. e non di associazione o fondazione (e che quindi non poteva avvalersi del provvedimento generale), di trattare i dati idonei a rivelare le convinzioni religiose degli studenti relativamente all'insegnamento della religione cattolica.

L'autorizzazione generale n. 3/1997, come già accennato, è scaduta il 30 settembre 1998 ed è stata sostituita dalla n. 3/1998, valida fino al 30 settembre 1999, che ha sostanzialmente riprodotto la precedente con limitate modifiche.

Poiché al momento dell'emanazione dei nuovi provvedimenti generali era in corso di approvazione in Parlamento la l. n. 344/1998, che ha procrastinato al 31 luglio 1999 il termine per l'adozione dei decreti delegati previsti dalla l. n. 676/1996 (i quali dovranno completare la disciplina sulla protezione dei dati personali, anche in attuazione delle raccomandazioni del Consiglio d'Europa), il Garante ha preferito,

come nella precedente occasione, evitare di dettare disposizioni di eccessivo dettaglio limitandosi a fissare i requisiti indispensabili per garantire la liceità dei trattamenti di dati sensibili e una idonea tutela degli interessati.

Raccogliendo l'indicazione fornita dal riferito caso dell'istituto scolastico privato, l'autorizzazione n. 3/1998 è stata resa applicabile agli istituti scolastici anche di tipo non associativo, per i trattamenti di dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per garantire il diritto degli studenti di scegliere se avvalersi dell'insegnamento della religione cattolica (art. 310, d.lg. 16 aprile 1994, n. 297).

Non si è invece ritenuto opportuno generalizzare l'indicazione fornita dall'autorizzazione speciale rilasciata alla Società Cattolica di Assicurazione rispetto a una fattispecie ritenuta estremamente particolare, il che ha ovviamente reso necessario rinnovare tale speciale autorizzazione alla scadenza.

L'attività del Garante si è poi incentrata sull'assistenza alle confessioni religiose in merito ai problemi interpretativi e applicativi della legge. Per tali motivi, nel corso dell'anno, sono stati ricevuti più volte i rappresentanti di talune confessioni religiose per l'esame di problematiche di carattere generale, alcune delle quali sono attualmente allo studio, dati gli inevitabili riflessi che determinate interpretazioni potrebbero avere su un elevato numero di persone in un settore così delicato.

Vi sono stati inoltre specifici interventi del Garante su questioni particolari sollevate da alcuni cittadini, anche se non attraverso un formale pronunciamento dell'Autorità.

Tra questi, ad esempio, va annoverata la precisazione sugli organi di stampa – da parte di un componente del Garante – nei confronti della notizia circolata nell'estate del 1998 sulla richiesta di una persona di essere cancellata dal registro dei battesimi. Il rappresentante dell'Autorità ha fatto notare che l'inserimento del nominativo di una persona nel registro dei battezzati costituisce l'attestazione di una vicenda «storica» che, in quanto tale, non può essere «cancellata».

Sempre nell'ambito degli interventi specifici, il Garante è stato spesso contattato (talvolta anche solo per conoscenza) da diversi cittadini i quali, in qualità di ex aderenti ad associazioni religiose, o semplicemente in quanto non interessati a ricevere da esse pubblicazioni e offerte, hanno esercitato i diritti previsti dall'art. 13 della l. n. 675/1996 richiedendo, il più delle volte, la cancellazione dei propri dati personali. Nella quasi totalità dei casi tali richieste hanno ricevuto una risposta affermativa e non hanno quindi richiesto il successivo intervento dell'Autorità.

Nel corso dell'anno, infine, è stata data risposta a un dipendente di un ospedale di proprietà di un istituto religioso, il quale aveva chiesto di conoscere se la norma del regolamento del personale, che impone di ispirare il comportamento anche esterno del dipendente «alla peculiare natura e finalità dell'ente da cui dipende l'ospedale», integrasse un'interferenza nella vita privata del dipendente medesimo.

A tale proposito il Garante, rilevato che obblighi di tal genere sono previsti per diverse categorie di dipendenti pubblici e privati, ha però precisato che potrebbero rinvenirsi eventuali rischi in sede di concreta applicazione di tali disposizioni. L'accertamento e la sindacabilità della lealtà e della correttezza della condotta dei dipendenti, infatti, devono essere effettuati nel rispetto delle norme poste a tutela della vita privata, come pure di altre disposizioni, anche di rango costituzionale, a garanzia delle libertà fondamentali.

2.6 SERVIZIO SANITARIO NAZIONALE

2.6.1 Profili generali

Le particolari garanzie previste dalla l. 31 dicembre 1996, n. 675 per il trattamento dei dati idonei a rivelare lo stato di salute che, come è noto, si inseriscono nella più generale categoria dei cd. «dati sensibili», hanno determinato qualche difficoltà sul piano dell'interpretazione, nonché dell'applicazione dei principi normativi della legge medesima nel settore sanitario.

Per questa ragione il Garante, in risposta ai numerosi quesiti posti da ospedali, professionisti o privati cittadini in cui sono state evidenziate le maggiori problematiche poste dalla nuova normativa, ha formulato una serie di pareri con i quali ha chiarito alcuni tra gli aspetti applicativi più controversi della disciplina in materia di protezione dei dati sulla salute.

Al tempo stesso, l'esame delle questioni pratiche più significative che si presentano in ambito sanitario a seguito dell'entrata in vigore della l. n. 675/1996 ha fornito a questa Autorità l'occasione per riflettere su alcuni aspetti della normativa che necessitano di un intervento integrativo e correttivo del legislatore delegato.

Tra le deleghe contenute nella l. n. 675/1996 esercitabili entro il 31 luglio 1999, una prima è mirata ad attuare, nel rispetto della direttiva comunitaria n. 95/46/CE, la Raccomandazione del Consiglio d'Europa n. 97 (5) del 13 febbraio 1997 sulla protezione dei dati sanitari, prevedendo anche eventuali forme di semplificazione della normativa in materia, sebbene nel rispetto dell'elevato livello di garanzia che presuppongono le informazioni sulla salute.

Attualmente il trattamento dei dati idonei a rivelare lo stato di salute è ancora disciplinato, in termini generali, dagli artt. 22 e 23 della l. n. 675/1996.

Come si ricorderà, la prima disposizione reca una norma generale che riguarda tutti i dati «sensibili», per i quali è richiesto il consenso scritto dell'interessato e l'autorizzazione del Garante. L'eccezione a questa regola, prevista per il trattamento dei dati sensibili da parte dei soggetti pubblici (art. 22, comma 3, l. n. 675/1996), aveva richiesto dall'origine l'introduzione di una norma transitoria che ha consentito ai soggetti pubblici di proseguire il trattamento per dodici mesi, previa comunicazione al Garante, anche in assenza di una espressa disposizione di legge che individui «i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite» (art. 41, comma 5, l. n. 675/1996). Tale termine, prorogato una prima volta dal d.lg. 8 maggio 1998, n. 135, è stato poi ulteriormente differito alla data dell'8 maggio 1999 (cfr. d.lg. 6 novembre 1998, n. 389).

È bene ricordare, parimenti, che l'art. 23 disciplina invece, in modo specifico, il trattamento dei «dati inerenti alla salute» da parte dei soli esercenti le professioni sanitarie e degli organismi sanitari pubblici, prevedendo per questi la possibilità di derogare alla regola generale della doppia condizione del consenso scritto dell'interessato e dell'autorizzazione del Garante, in due distinte ipotesi:

a) qualora si tratti di tutelare la salute e l'incolumità fisica dell'interessato, ovvero b) nel caso in cui le medesime finalità riguardino un terzo o la collettività.

Mentre nella prima ipotesi il trattamento può avere luogo anche senza l'autorizzazione del Garante, ma con il consenso scritto dell'interessato, nel secondo caso, in mancanza del consenso dell'interessato, devono essere rispettate le prescrizioni contenute nel provvedimento di autorizzazione n. 2/1998 emanato dal Garante (in G.U. del 1° ottobre 1998) (art. 23, comma 1, della l. n. 675/1996) o in altra speciale autorizzazione.

La complessa articolazione di questa disposizione, già evidenziata nella *Relazione per l'anno 1997*, ha riproposto alcuni dubbi che questa Autorità ha cercato di dirimere cogliendo anche questa occasione per stimolare alcune possibili semplificazioni delle procedure di applicazione della normativa in ambito sanitario.

In particolare, posto che gli esercenti le professioni sanitarie possono trattare i dati sulla salute dei propri pazienti soltanto dopo averne acquisito il consenso scritto (e purché questi siano stati preventivamente informati circa l'utilizzazione dei dati che li riguardano: artt. 23, comma 1, e 10 della l. n. 675/1996), il Garante ha precisato che tale consenso non deve essere necessariamente acquisito caso per caso, ma può essere richiesto anche *una tantum* in relazione al complesso delle attività che ciascun medico ritiene di dover porre in essere nei confronti dei propri assistiti.

L'informativa al paziente e la formula di consenso, ad esempio, possono riguardare, oltre alla normale attività di assistenza e cura, anche la possibilità per il medico di essere informato sulle condizioni di salute di un proprio assistito ricoverato presso una struttura ospedaliera (v. provvedimento del 12 ottobre 1998) o, ancora, di comunicare ai competenti organi dell'amministrazione finanziaria che effettuino un accertamento fiscale i dati personali (nome, diagnosi e cure applicate) contenuti nelle ricevute sanitarie (v. provvedimento del 31 dicembre 1998).

Nel corso dell'ultimo anno di attività, una particolare attenzione è stata inoltre dedicata al rapporto tra le disposizioni della l. n. 675/1996 e quelle della l. 5 giugno 1990, n. 135, in materia di prevenzione e lotta contro l'AIDS.

Con un provvedimento del 31 luglio 1998, il Garante è intervenuto tempestivamente a tutela del diritto di una dipendente pubblica che aveva chiesto di inibire alla competente commissione medica di comunicare al proprio ufficio di appartenenza la diagnosi di AIDS riscontrata in sede di accertamento sanitario ai fini del riconoscimento della dispensa dal servizio per inidoneità fisica all'impiego.

Dopo avere rilevato che la normativa in materia di protezione dei dati personali ha espressamente fatto salve alcune norme speciali previgenti, tra cui anche quelle sull'AIDS (art. 43, comma 2, l. n. 675/1996), il Garante ha esaminato il caso di specie chiarendo innanzi tutto che le disposizioni della l. n. 135/1990 prevalgono sulle norme regolamentari contenute nel d.m. n. 187/1997, le quali, pertanto, potranno essere applicate nella sola misura compatibile con le norme aventi forza di legge che tutelano la riservatezza e la dignità delle persone interessate.

L'art. 5 della l. n. 135/1990 sancisce «l'obbligo, per gli operatori sanitari che, nell'esercizio della loro professione, vengano a conoscenza di un caso di AIDS ovvero di un caso di infezione da HIV», di adottare «tutte le misure occorrenti per la tutela della riservatezza della persona assistita» e di comunicare i risultati degli accertamenti diagnostici «esclusivamente alla persona cui tali esami sono riferiti».

Con un primo provvedimento del 31 luglio 1998, con il quale si chiedevano elementi alla Commissione medica, il Garante ha ritenuto fondata la segnalazione e poiché sussisteva il concreto rischio di un pregiudizio rilevante a danno dell'interessata, ha vietato (art. 31, comma 1, lett. l) della l. n. 675/1996) alla Commissione medesima di comunicare a soggetti diversi dalla ricorrente i dati relativi all'accertamento dell'AIDS e all'infezione da HIV.

Nello stesso provvedimento il Garante ha segnalato la necessità di conformare il trattamento dei dati alla normativa in materia di protezione dei dati personali e, a tal fine, ha prospettato la necessità di modificare il regolamento approvato con il d.m. n. 187/1997, nella parte in cui questo prevede la trasmissione, all'amministrazione o all'ente che ha richiesto l'accertamento, di un processo verbale che rechi l'indicazione della diagnosi unitamente al grado di menomazione complessiva riscontrata (art. 6 del d.m. cit.).

Successivamente, con il provvedimento del 31 dicembre 1998, in risposta alla nota della Commissione medica che prospettava l'ipotesi di inserire nel verbale di accertamento la dicitura «omesso» in luogo del giudizio diagnostico di AIDS, il Garante ha rilevato che tale dicitura potrebbe, indirettamente, consentire a terzi di desumere la diagnosi relativa all'AIDS o all'infezione HIV, essendo tale caso, allo stato della legislazione vigente, l'unico nel quale il verbale di accertamento medico non può essere comunicato integralmente all'esterno.

Si è quindi suggerito che, nelle more delle auspicabili modifiche al d.m. sopra citato, la commissione medica provveda a inviare alle amministrazioni richiedenti, anziché copia del verbale di accertamento, un diverso attestato, privo di indicazioni diagnostiche, che certifichi semplicemente l'idoneità o no dell'interessato allo svolgimento dell'attività lavorativa.

Ancora a tutela della riservatezza dei pazienti affetti da AIDS, il Garante è intervenuto rispondendo a un quesito formulato dal primario ospedaliero di una divisione malattie infettive al quale un'azienda sanitaria locale, allo scopo di effettuare una rilevazione statistica sul consumo dei farmaci, aveva chiesto di fornire i nominativi dei pazienti ricoverati, affetti da AIDS, e altre indicazioni terapeutiche, quali il tipo di medicinali somministrati e la durata dei periodi di degenza.

Anche in questa occasione si è rilevato che la piena vigenza delle disposizioni della l. 5 giugno 1990, n. 135, e in particolare dell'art. 5 sopra citato, anche successivamente all'entrata in vigore della l. n. 675/1996, impone il rigoroso rispetto della riservatezza delle persone affette da AIDS e non consente, quindi, di effettuare rilevazioni sul numero dei ricoverati, sulla durata dei periodi di degenza e sul tipo di terapia cui gli stessi sono stati sottoposti, se non con modalità che garantiscano l'anonimato.

La tutela dell'anonimato dei pazienti affetti da HIV esige, peraltro, che l'accesso ai loro dati nominativi sia consentito esclusivamente al personale della divisione malattie infettive o di altri reparti ospedalieri che ne abbiano effettiva esigenza per ragioni di assistenza e di cura ai pazienti stessi. Questa Autorità ha segnalato pertanto la necessità, da un lato, di apprestare idonee misure di sicurezza che garantiscano un livello adeguato di protezione degli archivi elettronici in cui sono conservati i dati personali dei pazienti e, dall'altro, di limitare il trattamento alle sole operazioni strettamente pertinenti alle finalità di assistenza e cura dei pazienti stessi (v. provvedimento del 7 gennaio 1999).

Un'altra questione sulla quale il Garante, in più occasioni, è stato invitato a esprimere il proprio parere riguarda la possibilità, per le strutture ospedaliere, di fornire informazioni relative ai pazienti ricoverati presso le strutture stesse. Alcune aziende sanitarie, infatti, hanno chiesto se la semplice indicazione del reparto di degenza, potendo rivelare notizie sullo stato di salute delle persone ricoverate, rappresenti una violazione della normativa sulla protezione dei dati personali qualora non sia stata preventivamente acquisito il consenso scritto degli interessati.

In relazione a ciò il Garante ha chiarito di non ravvisare alcuna ipotesi di violazione, per un duplice ordine di considerazioni. In primo luogo perché, in virtù della norma transitoria di cui all'art. 41, comma 5, della l. n. 675/1996, i soggetti pubblici possono continuare a trattare i dati sensibili fino all'8 maggio 1999, anche in assenza dei presupposti indicati nell'art. 22, comma 3, della legge medesima, e indipendentemente dal consenso delle persone interessate. In secondo luogo perché si è rilevato che nell'ambito del servizio sanitario pubblico è previsto che parenti, conoscenti e organismi di volontariato accedano ai reparti ospedalieri per fare visita ai degenti, nel rispetto di determinati orari e delle eventuali modalità stabilite. La stessa «Carta dei servizi pubblici sanitari» (d.P.C.M. 19 maggio 1995) considera soltanto come

eccezione il fatto che un paziente possa chiedere di mantenere il riserbo circa la propria presenza nella struttura ospedaliera (v. provvedimento del 31 dicembre 1998 in Bollettino n. 6, in corso di stampa).

Di particolare rilievo è poi il provvedimento con il quale il Garante, in attuazione dei poteri attribuitigli dall'art. 31, comma 1, lett. l) della l. n. 675/1996, ha vietato il trattamento dei dati sulla salute di una donna le cui immagini radiografiche, unitamente ad altri dati clinici e all'indicazione del nome di battesimo e dell'età, erano state pubblicate su una rivista medica, senza che ne fosse stato preventivamente acquisito il consenso per iscritto.

Il Garante ha infatti ritenuto che tale pubblicazione sia espressamente vietata dalla legge (art. 23, comma 4, della l. n. 675/1996), in quanto costituisce diffusione di dati personali idonei a rivelare lo stato di salute. Considerato infatti che per «dato personale» si intende «qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale» (art. 1, comma 2, lett. c), della l. n. 675/1996) la pubblicazione suddetta, pur non riportando le complete generalità della persona cui l'immagine si riferiva, conteneva tuttavia elementi sufficienti a consentirne indirettamente l'identificazione (v. provvedimento del 21 dicembre 1998).

È stata fatta salva, in ogni caso, la possibilità di divulgare informazioni di carattere scientifico con altre modalità, nel rispetto della normativa in materia di protezione dei dati personali. Ad esempio l'utilizzo, nel caso sopra descritto, di un nome di fantasia o delle sole iniziali o di un codice numerico, garantendo l'anonimato dell'interessata, avrebbe permesso di contemperare le esigenze della ricerca medica e scientifica con il diritto alla riservatezza.

Viene in evidenza, infine, il problema della diffusione di dati sulla salute con specifico riferimento all'ambito sportivo. Sono pervenuti infatti a questa Autorità numerosi quesiti in ordine alla possibilità per le società sportive, di divulgare informazioni relative agli infortuni che determinano la temporanea interruzione dell'attività degli atleti.

A tale riguardo il Garante ha osservato che il divieto previsto dall'art. 23, comma 4, della l. n. 675/1996, non pregiudica il diritto dell'interessato di rendere pubbliche le proprie condizioni di salute, anche per interposta persona. Si è suggerito pertanto alle società sportive di acquisire da parte degli atleti, unitamente al consenso scritto per il trattamento dei dati sensibili, anche una apposita «delega» a rendere note alcune informazioni relative al proprio stato di salute, quando queste siano rilevanti per l'interesse pubblico che è sotteso alle attività agonistiche in cui gli atleti stessi si trovano impegnati, e a condizione che sia stata loro fornita, preventivamente, un'ideale informativa ai sensi dell'art. 10 della l. n. 675/1996.

Nello stesso provvedimento (22 giugno 1998) si è inoltre chiarito che i dati personali relativi a fenomeni di *doping* non possono essere considerati di per sé come dati «sensibili»; essi tuttavia possono assumere tale natura quando il loro trattamento, per la quantità e la qualità delle informazioni raccolte o per l'eventuale abbinamento con altri dati, comprenda o faccia emergere informazioni riguardanti lo stato di salute degli interessati.

La connotazione di «dato idoneo a rivelare lo stato di salute» è stata invece pienamente riconosciuta al giudizio di idoneità all'esercizio dell'attività agonistica, giacché esso indica in modo non equivoco la presenza di patologie nell'interessato o, comunque, la necessità di evitare i rischi connessi alla pratica agonistica. In questo

senso il Garante si è espresso in occasione del parere reso il 31 dicembre 1998 sulla bozza di modello unico di «libretto sanitario sportivo» predisposta dalla Consulta permanente per la medicina dello sport costituita presso il Ministero della sanità.

Si segnala infine la rilevanza, in ambito sanitario, dell'attività consultiva del Garante ai sensi dell'art. 31, comma 2, della l. n. 675/1996 (v. § 2.1.4 e 3.1.3).

2.6.2 «Sanitometro»

La posizione espressa dal Garante in occasione del varo del d.lg. 29 aprile 1998, n. 124, relativo alla «Ridefinizione del sistema della partecipazione al costo delle prestazioni sanitarie e del regime delle esenzioni, a norma dell'art. 59, comma 50, della l. 27 dicembre 1997, n. 449», è riassunta nel § 2.1.8 al quale si rinvia per brevità di esposizione.

2.6.3 Prescrizioni mediche

Gli sviluppi che si sono avuti ad inizio 1998 riguardo alla tematica della tutela della riservatezza dei dati riportati nelle prescrizioni mediche (e, in particolare, nelle ricette mediche), sono stati già riassunti anticipatamente nella *Relazione per l'anno 1997* (v. pagg. 38 e 81).

Al riguardo, il Garante ha avuto proficui contatti con il Ministero della sanità e con altri organismi competenti in materia in vista dell'attuazione della delega contenuta nella legge 8 aprile 1998, n. 94 (possibile attraverso i decreti delegati previsti dalla l. n. 676/1996).

2.6.4 Tessera sanitaria

Già da alcuni anni sono allo studio progetti di legge che prevedono l'introduzione di carte magnetiche quali strumenti destinati a sostituire appieno con transazioni elettroniche l'insieme dei documenti cartacei identificativi di un individuo o comunque a lui riferibili.

L'introduzione di tali strumenti ha alimentato un dibattito relativamente alle adeguate garanzie da introdurre a tutela del flusso di informazioni che l'utilizzo delle carte elettroniche comporta.

L'entrata in vigore della l. 31 dicembre 1996, n. 675, ha pertanto rappresentato l'occasione per riproporre le questioni relative alla protezione dei dati contenuti nei documenti elettronici, sulla base dei principi e dei criteri fissati dal legislatore e nell'ottica di un coordinamento con le iniziative assunte in ambito comunitario.

A tale riguardo vanno evidenziati alcuni progetti, di cui si discute anche in ambito G-7, che prevedono la realizzazione di carte sanitarie «interoperabili» a livello mondiale, cioè riconosciute e leggibili in ogni Paese per fare fronte alle emergenze e semplificare le procedure amministrative connesse all'erogazione di prestazioni sanitarie all'estero (progetti Eurocards e Netlink).

In ambito europeo la tessera sanitaria è stata già adottata in Germania, in Francia e in Belgio, e altri Paesi stanno elaborando progetti analoghi.

Anche l'Italia si è oramai avviata verso l'introduzione di questo strumento, per la cui realizzazione, prevista dalla stessa legge di accompagnamento alla finanziaria (art. 59, comma 50, lett. i), della l. 27 dicembre 1997, n. 449), il decreto-legge 28 dicembre 1998, n. 450, recentemente convertito (l. 26 febbraio 1999, n. 39), dispone interventi di carattere finanziario.

In particolare, sulla base di un progetto del Ministero della sanità, sono stanziati i fondi per l'avvio della sperimentazione della tessera sanitaria in un ambito territoriale limitato e in concomitanza con la sperimentazione del «sanitometro».

Il progetto infatti, che ha come obiettivo quello di definire i contenuti e di distribuire gradualmente sul territorio nazionale una carta elettronica sulla quale siano riportati i dati di carattere amministrativo e sanitario del cittadino, prevede una fase sperimentale da attuarsi in alcune regioni e nelle relative strutture del servizio sanitario nazionale (Asl, medici di base, farmacie, laboratori, ecc.), la quale dovrà concludersi entro il 30 giugno dell'anno 2000.

A partire da questa data la tessera sanitaria, dalla cui utilizzazione la legge di accompagnamento alla finanziaria prevede concreti risultati, anche in termini di razionalizzazione delle risorse e di contenimento della spesa sanitaria, dovrebbe essere distribuita a tutti i cittadini italiani per consentire il trattamento e la verifica dei dati sulla gestione delle prestazioni sanitarie.

Parallelamente, nelle diverse regioni sono in corso altri progetti di sperimentazione della carta sanitaria, approvati dal Ministero della sanità nell'ambito dei programmi speciali previsti dall'art. 12 del d.lg. 502/1992.

Questa Autorità ha fornito il proprio contributo agli uffici che stanno elaborando tali progetti, auspicando l'effettiva introduzione di garanzie adeguate per la tutela dei dati personali contenuti nella carta sanitaria. Si è così preso atto dell'ipotesi di proteggere tali dati tramite sistemi di cifratura che li renderebbero non accessibili da parte di operatori non autorizzati e della possibilità di prevedere, per il personale espressamente autorizzato all'accesso, vari livelli di autorizzazione.

2.7 PREVIDENZA E ASSISTENZA SOCIALE

2.7.1 Previdenza ed enti previdenziali

L'attività dell'Ufficio inerente alle tematiche connesse tanto alla previdenza quanto all'assistenza esercitate dai diversi enti, sia pubblici sia privati, non si è ancora attestata su volumi pari a quelli di altri settori interessati dall'impatto della normativa a tutela dei dati personali.

Si può affermare però che, pur essendo stati numericamente modesti, i casi nei quali gli enti gestori della previdenza hanno coinvolto l'Ufficio del Garante siano degni della massima attenzione in ragione dei contenuti di cui sono stati portatori.

Giova precisare, inoltre, che quesiti in materia previdenziale sono giunti all'Ufficio anche per il tramite di sedi distrettuali dell'Avvocatura generale dello Stato, nonché da diverse prefetture. Anche diversi liberi professionisti hanno richiamato l'attenzione dell'Ufficio su alcune specifiche problematiche.

Per quanto concerne l'oggetto delle richieste pervenute nel corso dell'anno, si possono distinguere alcune principali casistiche:

a) quesiti in merito all'attività di comunicazione dei dati ai patronati, alle associazioni di categoria e ai sindacati, attività, questa, in essere da tempo presso i principali enti previdenziali e che rappresenta per essi, ma soprattutto per gli iscritti, una netta facilitazione per la definizione delle posizioni assicurative dei singoli. Di tale problematica il Garante si è fatto carico allorché ha formulato alcuni suggerimenti al Governo relativi ai contenuti dell'emanando decreto legislativo sul trattamento dei dati sensibili nella pubblica amministrazione;

b) quesiti attinenti all'applicazione, da parte delle amministrazioni previdenziali, delle disposizioni contenute nella l. n. 241/1990 e nei relativi regolamenti di attuazione, in relazione a quanto sancito dalle norme sulla protezione dei dati personali sopraggiunte con la l. n. 675/1996;

c) segnalazioni relative a ipotesi di violazione della l. n. 675/1996 in materia di comunicazione e diffusione a terzi di dati personali, in alcuni casi anche sensibili;

d) comunicazioni all'Ufficio avvenute ai sensi dell'art. 41, comma 5 della l. n. 675/1996;

e) richieste di parere riferite a moduli predisposti ai fini di resa dell'informativa e dell'acquisizione, ove necessario, del consenso informato.

Nell'attività sopra descritta, l'Ufficio ha adottato criteri di collaborazione con gli enti previdenziali, allo scopo di agevolare il consolidarsi, quanto più rapido possibile, di soluzioni attuative al tempo stesso della l. n. 675/1996 e delle esigenze, manifestate dagli enti medesimi, di continua innovazione nell'erogazione delle prestazioni previdenziali e assicurative.

2.8 LAVORO E LEGISLAZIONE SOCIALE

Nell'ambito del rapporto di lavoro, uno dei trattamenti di dati personali più rilevanti è senza dubbio quello che riguarda i dati sensibili (si pensi a quelli relativi alle trattenute sindacali o idonei a rivelare lo stato di salute) che, come è noto, la l. n. 675/1996 rende lecito solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.

Il Garante si è avvalso anche in questo campo della possibilità di rilasciare un'autorizzazione generale che è stata rinnovata fino al 30 settembre 1999, con la quale ha esonerato i datori di lavoro privati, nonché gli altri titolari di trattamenti finalizzati alla gestione del rapporto di lavoro, dall'obbligo di richiedere singolarmente l'autorizzazione per il trattamento dei dati sensibili. Si è facilitata in tal modo la gestione dei rapporti di lavoro nel rispetto dei diritti e delle libertà fondamentali dei lavoratori dipendenti e autonomi (autorizzazione n. 1/1998 al trattamento dei dati sensibili nei rapporti di lavoro, G.U. del 1° ottobre 1998, n. 229).

Senza altri particolari mutamenti rispetto alla precedente autorizzazione, il nuovo provvedimento generale autorizza però, espressamente, il trattamento dei dati sensibili relativi all'adempimento di obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro. Un ulteriore elemento di novità consiste poi nell'aver previsto, tra le categorie di dati autorizzati, quelli relativi alla gravidanza, al puerperio e all'allattamento.

Sotto altro profilo, la complessa disciplina normativa concernente il trattamento dei dati personali nell'ambito del rapporto di lavoro, specie per quanto riguarda la tenuta delle liste dei lavoratori in mobilità da parte del Ministero del lavoro e della previdenza sociale e, ora, delle regioni, ha reso necessario uno specifico intervento (provv. del 12 ottobre 1998). In questa occasione il Garante ha constatato che la disciplina in materia (l. 23 luglio 1991, n. 223) non prevede espressamente la divulgazione delle liste di mobilità e che anche dopo la recente introduzione del Sistema informativo lavoro (d.lg. 23 dicembre 1997, n. 469) - che naturalmente incide sulla conoscibilità dei dati relativi ai lavoratori - è stata esclusa la pubblicità delle suddette liste in favore di privati (si pensi al singolo datore di lavoro) diversi dai soggetti autorizzati dal Ministero alla mediazione tra domanda e offerta di lavoro.

Su richiesta, poi, di una società autorizzata alla mediazione tra domanda e offerta di lavoro, il Garante ha espresso un articolato parere (prov. del 24 dicembre 1998) in merito agli adempimenti da porre in essere in relazione al trattamento dei dati nel settore del lavoro interinale.

In tale parere il Garante ha precisato che le società che operano nel campo del collocamento della manodopera e trattano i dati degli aspiranti e dei lavoratori assunti con contratto di lavoro temporaneo per essere utilizzati presso altre imprese, devono rispettare specifici obblighi per tutelare la riservatezza delle persone, senza per questo dover attivare complicate procedure.

A tal fine l'Autorità ha inteso non solo chiarire alcuni aspetti applicativi della l. n. 675/1996, ma ha fornito anche indicazioni generali e suggerito soluzioni operative affinché quanti operano nel settore del mercato del lavoro interinale possano adempiere correttamente alle disposizioni della legge con modalità semplificate e senza aggravii burocratici.

È stato infatti precisato che per poter raccogliere, conservare e utilizzare i dati contenuti nei *curricula vitae* è necessario fornire agli interessati una informativa che indichi i soggetti o le categorie di soggetti ai quali i dati verranno comunicati, e spieghi, tra l'altro, le modalità del trattamento e i diritti dell'interessato a conoscere, integrare, modificare, cancellare i dati raccolti. L'informativa, ha sottolineato in particolare il Garante, nel caso di trasmissione di *curricula* a mezzo posta o fax, potrebbe essere fornita ad esempio mediante l'utilizzo da parte dell'aspirante di un apposito modello, reso disponibile al pubblico, contenente un'informativa anche succinta, ma esauriente e comprensibile.

Il Garante ha anche precisato che per poter comunicare i dati dei candidati, l'agenzia dovrà acquisire il loro consenso (che deve essere scritto nel caso di dati sensibili) e specificare che tali informazioni verranno fornite alle sole imprese che chiederanno il *curriculum*.

Una ulteriore indicazione del Garante ha riguardato la possibilità, per la società che colloca manodopera, di raccogliere con un unico atto il consenso, sia per quanto riguarda il rapporto che intercorre tra essa e il lavoratore, sia per conto delle imprese utilizzatrici, con l'obbligo per queste ultime di trattare soltanto i dati strettamente necessari per l'offerta di lavoro.

Con il medesimo parere, questa Autorità ha ritenuto opportuno ribadire che anche in caso di raccolta di dati via Internet, le modalità devono comunque permettere al candidato di ricevere l'informativa prima della compilazione dei dati e di manifestare il consenso anteriormente alla loro trasmissione alla società, ricordando, peraltro, che per quanto riguarda le reti telematiche il Governo è stato delegato a individuare apposite modalità applicative della l. n. 675/1996.

2.9 RICERCA

2.9.1 Ricerca storica e archivi

La tutela delle persone in relazione al trattamento dei dati personali trova nella ricerca storica un terreno applicativo del tutto peculiare. Nello svolgimento dei propri studi, infatti, gli storici si trovano necessariamente a consultare ed elaborare una grande quantità di documenti contenenti dati personali. Di qui il problema di valutare in che misura e con quali modalità possa essere applicata a tali trattamenti

la disciplina disposta in via generale dalla l. 31 dicembre 1996, n. 675, in modo da operare in concreto un adeguato contemperamento tra la tutela della riservatezza e l'attività di ricerca.

a) Il legislatore ha avuto riguardo a queste esigenze. La l. n. 675/1996, infatti, nel dettare modifiche alla normativa vigente, ha voluto espressamente specificare che «restano ferme, in quanto compatibili, le vigenti norme in materia di accesso ai documenti amministrativi e agli archivi di Stato» (art. 43, comma 2). Parallelamente, la l. n. 676, dello stesso 31 dicembre, recando una delega al Governo - successivamente rinnovata dal Parlamento con la l. 6 ottobre 1998, n. 344, sino al nuovo termine del 31 luglio 1999 - tiene conto della necessità di adottare uno o più decreti legislativi al fine di disciplinare proprio le modalità di trattamento dei dati personali utilizzati a fini storici e di ricerca (art. 1, comma 1, lett. a)).

Il tenore delle disposizioni appena richiamate mostra, da un lato, che il legislatore aveva inteso garantire comunque una tutela di fronte a tali trattamenti, sebbene essi siano svolti in relazione ad avvenimenti anche molto risalenti nel tempo e si riferiscano spesso a persone non più in vita; dall'altro, che nell'ulteriore specifica disciplina sarebbe stato necessario tenere conto delle particolarità proprie di questo tipo di utilizzo dei dati personali.

Invero, il riconoscimento delle peculiarità di tale problematica non trae origine solo da una scelta del Parlamento italiano, ma trova fondamento e sostegno in un ampio lavoro di elaborazione a livello internazionale che ha portato già all'emanazione di importanti atti normativi. Al riguardo, sono da ricordare i «considerando» nn. 29 e 40 e l'art. 6 della direttiva 95/46/CE del 24 ottobre 1995, la quale ha rappresentato il principale parametro per il nostro legislatore nell'elaborazione della l. n. 675/1996. In particolare, la direttiva afferma che il trattamento di dati personali per scopi storici (oltreché statistici o scientifici) non deve essere ritenuto incompatibile con le varie finalità per le quali i dati sono previamente raccolti, purché gli Stati membri forniscano garanzie «appropriate», tali da impedire, in particolare, l'uso dei dati per l'adozione di misure o decisioni nei confronti di singoli. Inoltre, i trattamenti a fini storici (anche in questo caso analogamente a quelli statistici o scientifici) rientrano tra quelli che in presenza di «garanzie adeguate» possono permettere la conservazione per i medesimi fini di dati precedentemente utilizzati per altre finalità.

È da richiamare poi la corposa elaborazione effettuata in sede di Consiglio d'Europa, che aveva condotto dapprima alla raccomandazione n. R. (83) 10 adottata il 23 settembre 1983, uno degli atti normativi espressamente richiamati dalla l. n. 676/1996 quale parametro cui uniformare la nostra legislazione in materia; successivamente, alla Raccomandazione n. R (97) 18 sui dati raccolti e trattati per scopi statistici, e infine all'ormai imminente adozione di un più avanzato progetto di raccomandazione specificamente dedicato agli archivi.

In questo quadro, il Garante ha dedicato particolare attenzione alle tematiche relative ai trattamenti svolti in sede di ricerca storica, anche al fine di armonizzarne la disciplina con l'evoluzione normativa in materia di trasparenza e accesso ai documenti amministrativi, nonché con quella relativa ai trattamenti realizzati dai giornalisti e dagli altri soggetti che esercitano attività di informazione.

Sembra infatti ragionevole che la progressiva tendenza a estendere l'accessibilità da parte dei cittadini ai documenti detenuti dalla pubblica amministrazione debba trovare piena applicazione anche quando gli stessi documenti siano custoditi dall'amministrazione degli Archivi di Stato. In altri termini, un dato che era accessibile in base alla normativa sulla trasparenza amministrativa non può non continuare a esserlo quando viene riversato negli Archivi. Né appare giustificato che, a parità di

condizioni, uno storico si trovi in una posizione sfavorevole rispetto a quella del cittadino o del giornalista. Anzi, la consultabilità acquista particolare rilievo proprio per il suo normale collegamento con la finalità di pubblicare e divulgare le elaborazioni effettuate su tale materiale sotto forma di manifestazioni del pensiero. Naturale è, qui, il riferimento alla disciplina dei trattamenti svolti nell'esercizio di attività d'informazione, la quale trova applicazione in relazione non solo a quelli effettuati dai soggetti iscritti all'albo, ma anche ai trattamenti temporanei «finalizzati unicamente alla pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero» (art. 25 l. n. 675/1996, come modificato dal d.lg. 28 luglio 1997, n. 123 e dal d.lg. 13 maggio 1998, n. 171).

È chiaro, da un lato, che le esigenze di ricerca storica richiedono la conservazione dei dati per un periodo superiore a quello richiesto dalle originarie finalità per le quali erano stati raccolti; dall'altro, che gli storici si trovano a utilizzare i dati per finalità diverse da quelle originarie: la ricerca storica, appunto. Ciò, però, non contrasta necessariamente con le disposizioni sulla tutela dei dati personali dedicate ai dati storici - se adeguatamente interpretate alla luce delle considerazioni sin qui accennate - e in particolare con i principi sanciti dall'art. 9 della l. n. 675/1996, per quanto attiene al vincolo della conservazione dei dati in modo da consentire l'identificazione dell'interessato «per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi erano stati raccolti e successivamente trattati» (comma 1, lett. e)).

b) All'interno di questo processo di graduale adeguamento della normativa in materia, nella prima metà del 1998 il Garante ha partecipato a un gruppo di lavoro costituito presso l'Archivio centrale dello Stato - Ministero per i beni culturali e ambientali, con lo scopo, oltre che di provvedere all'organizzazione della Conferenza nazionale degli Archivi (Roma, 1-3 luglio 1998), anche di elaborare un primo progetto da cui sarebbero potuti scaturire i testi dei richiamati decreti previsti dalla l. n. 676/1996.

Si è così pervenuti a un primo progetto di decreto successivamente sottoposto al Consiglio dei ministri. L'articolato, dando attuazione alla delega prima richiamata, sanciva esplicitamente la non incompatibilità del trattamento dei dati personali ai fini di ricerca storica con gli scopi per i quali essi erano stati originariamente raccolti e successivamente trattati. Esso disponeva inoltre che - nel rispetto delle altre disposizioni della stessa l. n. 675/1996 - tale uso delle informazioni poteva essere effettuato anche oltre il periodo di tempo indicato dal richiamato art. 9, comma 1, lett. e) della legge.

Inoltre, provvedeva sia a modificare l'art. 21 del d.P.R. 30 settembre 1963, n. 1409 («Norme relative all'ordinamento e al personale degli Archivi di Stato»), con il quale sono disciplinati i limiti alla consultabilità dei documenti, sia a inserire un nuovo articolo *21-bis*, specificamente dedicato al trattamento dei dati personali ai fini di ricerca storica. Quest'ultimo prevedeva che i documenti contenenti dati personali conservati negli Archivi di Stato potessero essere trattati a fini di ricerca storica a prescindere dagli scopi per i quali essi erano stati originariamente formati e successivamente trattati; in tal modo intendeva armonizzare meglio la disciplina, a favore di chi conduca ricerche storiche, con il precetto dell'art. 15, comma 1 della l. n. 675/1996 che, seppure nel diverso contesto della sicurezza dei dati, considerando il «trattamento non conforme alle finalità della raccolta» come un rischio, potrebbe portare, sul piano teorico, a non tener conto che, invece, quel modo di trattare i dati d'archivio è, per così dire, connaturato proprio al lavoro dello storico

(conseguenza invero evitata già dall'art. 9, comma 1, lett. *b*) e *d*) della l. n. 675/1996, che permette di trattare i dati anche per finalità diverse da quelle perseguite al momento della raccolta, purché compatibili).

Relativamente ai dati sensibili e a quelli concernenti a taluni provvedimenti giudiziari (artt. 22 e 24 della l. n. 675/1996), lo stesso art. 21-*bis* consentiva la consultabilità decorsi quaranta anni dalla data del documento che li contiene. In tal modo, si aveva riguardo al fatto che la ricerca storica ha sempre più spesso per oggetto eventi vicini all'epoca presente, e si riduceva conseguentemente il periodo di settanta anni previsto dal vigente art. 21, comma 1, del citato d.P.R. per la consultabilità dei documenti genericamente individuati come «riservati relativi a situazioni puramente private di persone» o dei «documenti dei processi penali».

Allo stesso tempo, però, si introduceva una differenziazione per i dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, demandando a un codice deontologico l'individuazione di specifiche cautele (come tra breve si dirà) e arricchendo in tal modo la stessa disciplina prevista dalla l. n. 675/1996. Inoltre, coerentemente con quanto disposto per i giornalisti, si prevedeva che i dati potessero essere comunicati o diffusi dall'utente, qualora ciò fosse stato indispensabile per le finalità di documentazione e di ricerca storica, ovvero qualora essi si riferissero a fatti o a circostanze resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

c) Al fine di rendere sufficientemente flessibile tale disciplina, lo schema di decreto delegato aveva inoltre ritenuto che lo strumento più adeguato potesse essere rappresentato da un apposito codice di deontologia e di buona condotta degli utenti degli archivi, la cui accettazione sarebbe stata condizione per l'ammissione alla consultazione. Esso sarebbe stato promosso dal Garante, secondo le procedure e le modalità previste dall'art. 31, comma 1, lett. *h*) della l. n. 675/1996, e destinato, appunto, agli utenti in senso lato, nella consapevolezza dell'impossibilità di considerare gli storici come una categoria professionale definita, al pari delle altre nell'ambito delle quali l'Autorità è chiamata a promuovere simili codici.

A tale fonte sarebbe stata demandata, fra l'altro, l'individuazione delle norme di correttezza e di non discriminazione da osservare nella comunicazione e nella diffusione dei documenti contenenti dati personali, nonché delle cautele da osservare per la consultazione e la diffusione di documenti contenenti dati idonei a rivelare lo stato di salute, la vita sessuale e i rapporti riservati di tipo familiare.

Sempre attraverso il medesimo art. 21-*bis*, si disciplinava anche l'esercizio dei diritti dell'interessato previsti dall'art. 13 della l. n. 675/1996 in relazione ai documenti detenuti presso gli Archivi di Stato. Al riguardo, si stabiliva che questi dovevano essere conservati per tali finalità e restare liberamente consultabili, qualora ciò fosse risultato necessario per motivi di documentazione o di ricerca storica. A tutela degli interessati veniva però prevista anche la possibilità che fosse disposto il blocco dei dati. Ciò, nel caso in cui il loro trattamento avesse comportato un concreto pericolo di lesione della dignità, della riservatezza o dell'identità personale degli interessati, oppure qualora i dati non avessero rivestito un particolare interesse pubblico.

Infine, si sanciva il principio che l'autorizzazione alla conoscenza di un dato da parte di un utente doveva considerarsi accordata, sussistendo le medesime condizioni, a ogni altro richiedente, in modo da garantire il rispetto del principio di uguaglianza anche in rapporto a dati o documenti detenuti da soggetti diversi.

d) Questo il quadro normativo che si andava delineando. Tuttavia esso non si è concretizzato definitivamente in quanto il decreto legislativo del 22 luglio 1998, che conteneva le disposizioni appena illustrate, non è stato, come si è riferito, emanato. Ciò però non ha impedito di proseguire gli approfondimenti, specie nell'ambito

della Commissione consultiva di seguito citata, la quale ha affiancato all'esame delle questioni relative all'accesso a singole fonti uno studio del più generale rapporto tra privacy e ricerca storica, studio che ha offerto anche alcune riflessioni utili per la futura normativa. Manca ancora, quindi, una disciplina compiuta delle modalità di trattamento dei dati personali utilizzati a fini storici.

Di ciò ha dovuto tener conto il Garante quando ha formulato il parere del 31 dicembre 1998, richiesto in relazione agli adempimenti prescritti dalla l. n. 675/1996 per la pubblicazione e la diffusione via Internet di una raccolta di corrispondenza indirizzata a una personalità di spicco della letteratura italiana di questo secolo.

L'Autorità, nelle more dell'emanazione dei decreti delegati di cui si è detto, ha ritenuto che il caso sottoposto potesse trovare soluzione sulla base del disposto del già citato comma 4-bis dell'art. 25 della l. n. 675/1996, relativo ai trattamenti effettuati dai giornalisti. Pertanto, la pubblicazione dell'epistolario in questione ha potuto esser ricompresa nell'ampia nozione di trattamento finalizzato «esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero», con la conseguenza di esentare i curatori della raccolta dalla necessità di acquisire il consenso degli interessati. Contemporaneamente, il Garante ha ritenuto applicabili le norme della legge n. 675 in tema di pubblicazione di saggi e articoli giornalistici anche in corso di diffusione attraverso reti telematiche, data anche l'assenza di una regolamentazione specifica in materia.

Si è potuto così adempiere al dovere dell'informativa agli interessati, attraverso la predisposizione, in premessa alla pubblicazione, di un'informativa semplificata volta a specificare l'identità del curatore dell'epistolario, nonché l'indirizzo al quale fare riferimento per l'eventuale esercizio dei diritti di cui all'art. 13 della l. n. 675/1996. Ciò in analogia con quanto disposto dal codice deontologico dei giornalisti pubblicato nella «Gazzetta Ufficiale» del 3 agosto 1998.

Tutto ciò, però, nel presupposto che chi utilizza i dati storici, pur rispettando l'integrità dei testi, provveda sempre a una preventiva valutazione dell'opportunità di eliminare i dati non necessari, specie quando questi siano idonei a rivelare i dati sensibili di cui all'art. 22 della l. n. 675/1996.

e) Un particolare versante applicativo dei principi posti a protezione dei dati personali è rappresentato infine dalle sedi in cui viene compiuta una valutazione in ordine alla possibilità di consentire la consultazione di documenti a carattere riservato conservati presso gli archivi di Stato e degli enti pubblici. Come è noto, in base alla legislazione archivistica, in via di modifica, tali documenti relativi alla politica estera o interna dello Stato, oppure a situazioni puramente private di persone, diventano consultabili, rispettivamente, 50 o 70 anni dopo la loro data; i termini, però, possono essere ridotti se la consultazione è richiesta per motivi di studio; la decisione al riguardo fa capo al Ministro dell'interno (d.P.R. 30 settembre 1963, n. 1409, art. 21 cit.).

In ordine a questa competenza, il Garante è stato chiamato a far parte della «Commissione consultiva per le questioni inerenti alla consultabilità degli atti di archivio riservati», che il Ministro dell'interno ha istituito per avvalersene «nell'analisi comparativa dell'interesse alla accessibilità degli atti della pubblica amministrazione e di quello a tutela della riservatezza personale, nella prospettiva del riconoscimento delle esigenze della ricerca storica» (d.m. 2 luglio 1998).

2.9.2 Ricerca scientifica e statistica

In attesa di definire in modo complessivo la disciplina della protezione dei dati personali nel settore della ricerca scientifica e statistica, tramite il recepimento delle raccomandazioni del Consiglio d'Europa R. (93) 10 e della più recente R. (97) 18, si sono registrate nel corso del 1998 una serie di importanti iniziative utili a delinearne il quadro.

Il Garante ha seguito con attenzione il dibattito sul tema partecipando attivamente a convegni, promuovendo incontri con le categorie interessate, rilasciando pareri su progetti o schemi di norme, rispondendo a quesiti formulati da cittadini o enti interessati.

Per quanto concerne l'attività di ricerca scientifica e tecnologica, il d.lg. 5 giugno 1998, n. 204, al fine di promuovere e sostenere la ricerca, riconosce alle pubbliche amministrazioni e alle università la possibilità di comunicare e diffondere dati relativi ad attività di studio e di ricerca, con esclusione di quelli sensibili o relativi a provvedimenti giudiziari.

Sotto tale aspetto è da ricordare ancora il citato schema di decreto legislativo approvato dal Governo il 22 luglio u.s. che aveva a oggetto anche la statistica.

In proposito, il Garante ha rilevato che tale schema, pur contenendo alcune disposizioni che incrementano l'attuale livello di protezione, non appariva idoneo ad assicurare il livello reso necessario dal nuovo contesto europeo e dai principi di delega della l. n. 676/1996.

Tra le iniziative parlamentari in corso e che in qualche modo toccano la materia è da annotare poi anche la proposta di legge n. 4023-A che propone modifiche alla disciplina e al funzionamento del Sistema statistico nazionale.

Fra le attività poste in essere invece dal Garante per promuovere la conoscenza tra il pubblico delle norme che regolano la materia, sono da menzionare, in particolare, alcune risposte ai quesiti pervenuti. Il Garante ha colto infatti queste occasioni per porre in evidenza taluni principi presenti nella l. n. 675/1996, o in altre leggi, segnalando a chi opera per scopi di ricerca scientifica o di analisi statistica l'esigenza di adeguare i tradizionali metodi di attività alla protezione dei dati personali.

In risposta a un quesito posto da un ente universitario circa la possibilità di fornire all'Istat l'elenco dei laureati nell'anno accademico 1996, il Garante ha anzitutto ricordato che il d.lg. 6 settembre 1989, n. 322 - fatto salvo dalla l. n. 675/1996, art. 43, comma 2, in quanto compatibile con la nuova disciplina sulla protezione dei dati - obbliga i soggetti pubblici a fornire i dati loro richiesti per le rilevazioni previste dal Programma statistico nazionale, con esclusione di quelli relativi a razza, opinioni politiche, religione, salute, vita sessuale e condanne penali. In tale quadro normativo è stata considerata quindi lecita la trasmissione di dati per una indagine rientrante nel Programma statistico nazionale (art. 27, comma 1, l. n. 675/1996). Il Garante ha poi evidenziato che la trasmissione dei dati non avrebbe trovato ostacoli nel caso in cui non fosse stata inserita in tale Programma, stante il disposto del sopracitato d.lg. 5 giugno 1998, n. 204 che favorisce la pubblicità dei dati relativi ai laureati.

Pare utile citare poi il parere fornito dal Garante a uno studente universitario circa la possibilità di acquisire - per lo svolgimento di una tesi di laurea - alcuni dati statistici di carattere giudiziario relativi a una comunità zingara ben individuata.

In questo caso il Garante, pur constatando l'esistenza della finalità di carattere scientifico della ricerca, ha rilevato che la comunicazione dei dati non poteva ritenersi legittima in quanto il campione circoscritto di informazioni da analizzare rendeva i dati anonimi solo in apparenza, essendo i soggetti comunque identificabili.

Nel corso del 1998 il Garante ha rilasciato anche un parere sulle rilevazioni rientranti nel Programma statistico nazionale per il triennio 1998-2000, comprendenti anche le condizioni di salute e il ricorso a servizi sanitari, rilevando che tali indagini, poiché avviate dall'Istat fin dal 1980, possono essere effettuate in virtù della norma transitoria contenuta nell'art. 41, comma 5, della l. n. 675/1996.

Da ultimo è da segnalare il parere fornito dal Garante riguardo a una richiesta di autorizzazione pervenuta da un Istituto privato, volta ad accedere ai dati anagrafici degli studenti di una fondazione scolastica per poter effettuare una ricerca epidemiologica.

Il Garante, nel sottolineare che per la trasmissione di dati tra soggetti privati la legge non prevede autorizzazioni, ha rilevato che la comunicazione dei dati «comuni» per tali finalità è possibile con il consenso degli interessati o in presenza di uno degli altri requisiti previsti dall'art. 20 della l. n. 675/1996 (ad esempio: pubblicità di alcuni registri, necessità di adempiere a un obbligo previsto da una norma), o qualora i dati trattati siano anonimi (art. 21, comma 4, lett. a)).

2.9.3 Ricerca medica ed epidemiologica

Per quanto concerne in particolare gli atti normativi in grado di incidere sulla protezione dei dati personali nel campo della ricerca medica, è da citare la l. 8 aprile 1998, n. 94 (legge di conversione del cd. «decreto Di Bella») recante «disposizioni urgenti in materia di sperimentazioni cliniche in campo oncologico e altre misure in materia sanitaria», che afferma il principio del consenso informato e del rispetto della dignità e della riservatezza del paziente. Inoltre, con il d.P.R. 20 ottobre 1998, n. 403 in materia di semplificazione delle certificazioni amministrative, si è proceduto a riformulare le modalità per la rilevazione dei dati statistici di base relativi agli eventi di nascita, comprensivi dei dati inerenti ai nati con malformazioni o ai morti.

Nel corso del 1998 si è assistito a interessanti iniziative che hanno portato allo studio di alcuni Codici di deontologia e di buona condotta.

La l. n. 675/1996 vede con favore l'adozione di tali codici che possono contribuire ad accrescere il livello di protezione dei dati personali.

Indicazioni in tal senso sono rinvenibili anche nel nuovo codice di deontologia medica emanato lo scorso ottobre. È stato inoltre avviato un dibattito sulla proposta per un codice di autodisciplina del trattamento dei dati sensibili nel settore dell'epidemiologia. L'adozione di codici è stata auspicata tramite la valorizzazione del ruolo delle associazioni scientifiche e degli organi governativi competenti nella Quarta conferenza nazionale di statistica tenutasi a Roma dall'11 al 13 novembre, nonché in un seminario organizzato anch'esso a Roma il 17 dicembre 1998 dalla Scuola di formazione del personale addetto alla gestione delle Istituzioni e degli enti pubblici di ricerca e sperimentazione.

A livello internazionale è da segnalare infine che durante la 20ª Conferenza sulla protezione dei dati tenutasi a Santiago de Compostela, dal 16 al 18 settembre scorso (v. cap. 4.6), i rappresentanti delle Autorità garanti dei Paesi dell'Unione europea e dello Spazio economico europeo hanno espresso gravi preoccupazioni sulla proposta del Governo islandese di creare una banca dati contenente informazioni relative alla salute, comprensive dei dati di carattere genetico dell'intera popolazione.

La richiesta di riconsiderare il progetto è stata dettata dal pericolo di un allargamento delle originarie finalità del registro per interessi commerciali nonché dalla consapevolezza che il rischio di identificare il singolo, considerata anche la particolare natura dei dati, aumenta notevolmente in un Paese con una popolazione relativamente scarsa.

2.10 ISTITUTI DI CREDITO E ASSICURAZIONI

Il settore bancario e quello assicurativo sono stati coinvolti in modo rilevante dall'applicazione delle disposizioni sul trattamento dei dati personali. La l. n. 675/1996 ha infatti introdotto precise regole giuridiche a tutela della riservatezza delle persone, che hanno integrato e rafforzato le misure e gli accorgimenti che venivano adottati già dagli operatori di questi settori per garantire la segretezza e la confidenzialità delle informazioni personali acquisite nei rapporti con la clientela.

I problemi maggiori riscontrati dalle banche e dalle assicurazioni, anche nell'anno 1998, sono derivati dalla gestione degli adempimenti relativi all'*informativa* e al *consenso* (v. la *Relazione per l'anno 1997*, cap. 4.4., pagg. 72 e ss.).

In quest'anno il Garante ha svolto un'intensa attività di verifica sul pieno rispetto dei principi già affermati in precedenti provvedimenti, soprattutto per quanto riguarda il settore creditizio e finanziario (v. cap. 2.2).

Tale settore è stato interessato da un'apposita indagine conoscitiva, che l'Ufficio ha svolto chiedendo informazioni a numerosi istituti di credito e che ha riguardato oltre 800 modelli sottoposti ai clienti delle diverse banche. Al tempo stesso, l'Autorità ha continuato l'attività di consultazione, anche nell'ambito di specifici gruppi di lavoro, con le principali istituzioni e società bancarie.

In sintesi si è appurato che, a seguito delle indicazioni generali fornite dal Garante, i cui contenuti sono stati ampiamente riportati sulla stampa, varie società operanti nel settore hanno riformulato i modelli già distribuiti ai propri clienti, inviandoli nuovamente a tutta la clientela.

La modulistica distribuita dalle banche, per quanto complessa e non facilmente comprensibile per il cittadino, è apparsa in buona parte conforme ai principi evidenziati dall'Autorità, avendo previsto di regola la possibilità per la clientela di esprimere il proprio consenso «informato» nei riguardi dei trattamenti anche non strettamente connessi ai servizi richiesti contrattualmente (in riferimento, ad es., all'invio di materiale pubblicitario e, in genere, all'offerta di prodotti e servizi anche di società terze), senza che ciò abbia alcun riflesso sul contratto medesimo.

Tuttavia, l'Autorità ha constatato che diversi clienti non hanno ancora dato riscontro ai modelli inviati dalle banche e dalle altre società operanti nel settore.

Il problema del mancato ritorno del consenso è stato fronteggiato temporaneamente con la soluzione già prospettata nel 1997 dal Garante in base alla quale, nell'eventuale attesa del rilascio della dichiarazione relativa al consenso, la richiesta di una prestazione da parte del cliente (es.: l'emissione di un assegno, il bonifico bancario) può essere considerata come una manifestazione di volontà equiparabile al consenso per le operazioni di trattamento connesse a quella prestazione, sia pure in via del tutto provvisoria.

Trattandosi di soluzione transitoria, vi è pertanto la necessità che la clientela rimasta inerte sia nuovamente stimolata a esprimere il proprio consenso, in modo da arrivare a una piena regolarizzazione dei trattamenti di dati svolti dagli istituti di credito.

Il Garante stesso, nei primi mesi dell'anno, si è impegnato a formulare schemi di modelli che, pur mantenendo ferme le sostanziali garanzie a tutela dei diritti degli interessati, siano più semplici e meglio comprensibili, in modo da permettere ai clienti di fornire più agevolmente un rapido riscontro alle richieste di consenso formulate dalle società bancarie.

Un primo nuovo schema di informativa e di consenso è stato messo a punto alla fine del 1998, e nei primi giorni di febbraio 1999 l'Autorità, considerato il generale interesse alla tematica, ha ritenuto opportuno renderlo pubblico attraverso gli organi di informazione, sottoponendolo all'attenzione degli istituti di credito, degli utenti e dei loro organismi rappresentativi, anche per avere loro osservazioni e suggerimenti.

Essendosi conclusa l'analisi delle osservazioni pervenute, il Garante trasmetterà il nuovo modello revisionato a tutti gli operatori del settore bancario, che comunque hanno intenzione di inviare alla clientela un opportuno messaggio di richiamo (inserito, in particolare, negli estratti conto).

È evidente che lo schema di modello potrà essere utile anche per altri settori economici, finanziari e produttivi, come appunto quello delle assicurazioni, che hanno spesso riscontrato problemi analoghi a quelli delle banche e hanno più volte chiesto all'Autorità, per il tramite dell'associazione di categoria (ANIA), di avere precise indicazioni al fine di rendere più comprensibile la modulistica già distribuita ai propri clienti.

Una problematica particolarmente delicata affrontata dagli operatori del settore bancario e assicurativo è senz'altro quella del trattamento dei dati aventi natura sensibile (stato di salute, opinioni sindacali o politiche, ecc.).

In attesa delle precise indicazioni che verranno fornite nei decreti delegati previsti entro la fine di luglio 1999, sono applicabili al riguardo le regole più generali previste dalla l. n. 675/1996 (consenso scritto degli interessati, previa autorizzazione del Garante: art. 22, comma 1). Sotto questo profilo, l'Autorità ha rinnovato quest'anno, con alcune lievi modifiche, le autorizzazioni generali già rilasciate nel 1997 per il trattamento di questi dati (v. § 3.1.3), tenendo presenti anche talune particolari esigenze evidenziate dagli operatori (è stata, ad esempio, rilasciata una specifica autorizzazione a una società cooperativa di assicurazione che, a livello statutario, prevede per i propri soci la professione di determinate convinzioni religiose).

Per quanto riguarda, poi, altri temi specifici relativi alla tutela dei dati personali, occorre di seguito soffermare brevemente l'attenzione su alcuni provvedimenti dell'Autorità che rivestono maggiore interesse soprattutto per il settore bancario e finanziario.

L'Autorità ha anzitutto esaminato, a seguito di alcune segnalazioni, la questione del rispetto della cd. distanza di cortesia presso gli sportelli degli istituti di credito (già nota alle banche e, in parte, disciplinata attraverso il Codice di comportamento del settore bancario e finanziario adottato dall'ABI).

Al riguardo il Garante ha evidenziato che, anche in virtù delle disposizioni previste dalla l. n. 675/1996 in materia di sicurezza dei dati personali, le banche devono adottare ogni utile iniziativa per garantire la distanza di cortesia, la quale rappresenta una misura opportuna per prevenire l'impropria conoscenza da parte di terzi delle informazioni eventualmente fornite dal cliente all'operatore di sportello.

L'Autorità garante è dovuta intervenire anche relativamente al cd. *benefondi*, ossia in ordine alla prassi consolidata nell'attività bancaria, basata su accertamenti anche informali, attraverso i quali viene garantita l'esistenza presso la banca di fondi sufficienti a coprire gli assegni emessi. L'intervento si è reso necessario perché, secondo le numerose segnalazioni pervenute all'Ufficio, talune banche si sono rifiutate in nome della *privacy* di rilasciare il *benefondi* su assegni emessi dai propri clienti.

Il Garante, che si era già espresso sull'argomento in precedenti occasioni, ha affermato che la l. n. 675/1996 non ha introdotto alcun divieto nei confronti del *benefondi*. Queste informazioni possono essere fornite dagli istituti di credito nel rispetto dei principi generali che la legge stessa prevede per tutti i trattamenti di dati personali svolti dalle banche e secondo le indicazioni generali riportate nei modelli di informativa e di richiesta del consenso distribuiti alla clientela (nelle quali rientra anche questo tipo di operazione necessaria per una corretta esecuzione del rapporto bancario). Si è comunque sottolineata l'esigenza che la prassi del *benefondi* sia svolta correttamente e che le informazioni siano fornite ai soli soggetti legittimati all'incasso o alla negoziazione dell'assegno e non a estranei.

Sempre in ambito bancario, alcune associazioni dei consumatori e diversi cittadini hanno chiesto all'Autorità di verificare la legittimità dell'attività svolta da una società che gestisce carte di credito e di pagamento, la quale, secondo la segnalazione, avrebbe inviato alla propria clientela, con l'estratto conto mensile, materiale pubblicitario non richiesto dai titolari delle carte, ai quali sarebbero stati addebitati, invece, i relativi costi di spedizione.

Anche in questo caso il Garante ha avuto modo di precisare che la l. n. 675/1996 non ha introdotto un divieto generalizzato nei confronti della raccolta e dell'utilizzazione dei dati personali per finalità commerciali o di *marketing*, ma ha individuato, piuttosto, i presupposti fondamentali sulla base dei quali è possibile effettuare tali operazioni - presupposti che sono in buona parte comuni agli altri trattamenti di dati effettuati nel settore (in particolare, l'informativa e, ove necessario, la richiesta del consenso).

Si è inoltre ricordato che la direttiva comunitaria n. 95/46/CE e la l. n. 675/1996 recano alcune norme transitorie che rendono al momento possibile non richiedere il consenso degli interessati qualora il trattamento riguardi dati raccolti prima dell'8 maggio 1997 (data di entrata in vigore della legge stessa), o sia iniziato anteriormente a tale data (sempre che il soggetto che tratta i dati non li divulghi a terzi: v. art. 41, comma 1). Questa disciplina transitoria non preclude però alla persona interessata di avvalersi dei nuovi diritti previsti dall'art. 13 della l. n. 675/1996, chiedendo alla stessa società «titolare del trattamento» (o al soggetto da essa designato come «responsabile») l'immediata cessazione delle operazioni collegate all'invio di materiale pubblicitario, ovvero al compimento di operazioni di *marketing*.

Per quanto riguarda gli aspetti di propria competenza, il Garante ha constatato che la società ha provveduto, anche sulla scorta delle indicazioni fornite nel 1997 dalla stessa Autorità, a inviare ai titolari di carte di credito l'informativa e la richiesta del consenso, prevedendo specifiche opzioni. Tra esse, appunto, quella concernente il trattamento dei dati a fini di informazione e promozione di prodotti o servizi, mediante annunci inseriti nelle comunicazioni periodiche ai titolari. Tale procedura sarebbe stata quindi seguita anche nei riguardi di clienti i cui dati sono stati acquisiti e trattati, anche a scopo pubblicitario, prima dell'entrata in vigore della legge.

L'invio da parte della società di materiale commerciale relativo anche a società terze non comporta, di per se stesso, una comunicazione a tali società dei nominativi e degli indirizzi dei titolari delle carte di credito e non rende al momento necessario raccogliere il consenso dei clienti nei cui confronti tale trattamento sia iniziato prima dell'8 maggio 1997. A diversa conclusione si dovrebbe semmai pervenire nella circostanza, non segnalata all'Ufficio, in cui risultasse una comunicazione dei dati relativi ai clienti rivolta alle società terze alle quali si riferisce la pubblicità inserita negli estratti conto.

L'Autorità ha infine ricordato agli interessati che la società che gestisce le carte di credito ha comunque dichiarato che esaudirà scrupolosamente le eventuali richieste della clientela che non intenda più ricevere materiale pubblicitario riferito anche a società terze, a prescindere dal fatto che gli stessi abbiano eventualmente manifestato un precedente consenso al riguardo.

Più in generale, per ciò che attiene alle problematiche del *direct marketing*, si osserva che, dagli accertamenti effettuati in ambito bancario e finanziario, una parte della clientela ha manifestato, sulla base della modulistica distribuita, un diniego nei riguardi dell'utilizzo dei dati per l'invio di materiale diverso da quello legato al servizio richiesto a livello contrattuale.

In ogni caso, per risolvere le predette problematiche, l'Autorità ha avviato alcune procedure di consultazione con gli operatori del settore e le principali istituzioni finanziarie, il cui lavoro potrebbe essere utile anche in sede di predisposizione da parte del Governo del decreto legislativo che dovrà dettare regole specifiche per questa materia, recependo anche le linee guida indicate nella raccomandazione del Consiglio d'Europa n. R. (85) 20, del 25 ottobre 1985, sui dati utilizzati per fini di *direct marketing*.

2.11 INTERMEDIAZIONE FINANZIARIA

Un problema di tutela dell'interessato di fronte al trattamento di dati personali compiuto da terzi, si può porre, naturalmente, anche con riguardo all'attività di intermediazione finanziaria.

Ciò anzitutto perché, per sua natura, l'attività di prestazione di servizi di investimento e accessori può essere svolta al meglio dall'intermediario soltanto a condizione di avere piena cognizione di talune informazioni di carattere personale (situazione patrimoniale, propensione al rischio, ecc.), che devono essere richieste al risparmiatore (art. 28, reg. CONSOB 1° luglio 1998, n. 11522). In altre parole, ferma restando la possibilità del rifiuto di fornire i dati, sono gli stessi caratteri dell'attività in questione a esprimere il principio del *know your customer* così definito dalla Corte di Cassazione in una recente sentenza (14 novembre 1997, n. 11279).

I dati richiesti possono avere anche carattere sensibile e avendo presente questa non rara ipotesi il Garante ha perciò incluso gli intermediari finanziari (assumendone un'accezione ampia) tra i destinatari dell'autorizzazione generale n. 5 del 1998. Per effetto di essa, a detti soggetti è quindi consentito il trattamento dei dati sensibili di cui all'art. 22, comma 1, della l. 31 dicembre 1996, n. 675, fatta eccezione per i dati idonei a rivelare la vita sessuale.

Per altro verso, nel settore in esame si pone anche un problema di tutela della riservatezza di taluni soggetti che operano dal lato dell'offerta di prodotti finanziari. Per il corretto funzionamento del mercato finanziario, infatti, è essenziale che i potenziali investitori siano in grado di conoscere la maggior quantità possibile di informazioni relative alle società che vi operano, allo scopo di potere compiere quelle che la normativa vigente chiama «consapevoli scelte di investimento».

Tra queste informazioni è evidente che possono assumere grande importanza, nell'apprezzamento del pubblico, anche quelle relative, a seconda dei casi, all'onorabilità, alla professionalità o ai compensi percepiti dagli esponenti aziendali (amministratori, sindaci, ecc.). Al riguardo, però, ognuno intende che simili soggetti hanno, per contro, interesse a non essere esposti ingiustificatamente, e in ogni caso non oltre il necessario, alla curiosità altrui.

In merito il Garante ha avuto occasione di pronunciarsi più volte, nel corso del 1998 (v. il provvedimento del 10 febbraio 1998 relativo all'ISVAP, nonché quello del 18 novembre 1998, relativo all'art. 32 del reg. CONSOB 1° luglio 1998, n. 11520), sancendo l'importante principio secondo il quale il diritto dei potenziali investitori di conoscere le predette informazioni prevale sulle esigenze di riservatezza degli esponenti aziendali, a patto che il sacrificio sia autorizzato da un'idonea fonte normativa (nel minimo un regolamento, non essendo invece sufficiente un mero decreto ministeriale).

Al riguardo si veda anche la pronuncia del 16 febbraio 1999 (di cui si è già detto nel § 2.2.3) nella quale il Garante ha esaminato la nozione di «attività economiche» al fine di chiarire l'ambito di applicazione delle disposizioni della l. n. 675/1996 (artt. 12, comma 1, lett. *f*) e 20, comma 1, lett. *e*) che prevedono, quale ipotesi di esclusione del consenso dell'interessato, il trattamento che «riguardi dati relativi allo svolgimento di attività economiche».

Al di là dei riscontri concreti, che nel numero vanno ben oltre quelli qui ricordati, è in ogni caso agevole prevedere che il settore dell'attività di intermediazione finanziaria sia tra quelli che maggiormente alimenteranno il dibattito scientifico e il contenzioso amministrativo negli anni a venire, in considerazione del suo grado crescente di complessità e di ricchezza di implicazioni.

2.12 INFORMATICA E TELECOMUNICAZIONI

2.12.1 Telefonia e servizi di telecomunicazioni

L'universo delle telecomunicazioni e, al suo interno, il settore della telefonia ha costituito oggetto di particolare attenzione da parte del Garante nel corso del 1998, sia per le innovazioni legislative che hanno contraddistinto questo ambito, sia per le molte segnalazioni pervenute in merito, che dimostrano la particolare sensibilità dell'opinione pubblica.

2.12.1.1 La nuova normativa di tutela nelle telecomunicazioni

Le innovazioni più significative in materia di protezione della vita privata nel settore delle telecomunicazioni sono state introdotte in Italia con il d.lg. 13 maggio 1998, n. 171, a cui si era fatto già cenno nella *Relazione per l'anno 1997* (con particolare riguardo alla descrizione del provvedimento adottato dal Garante sull'obbligo, previsto dal d.P.R. n. 318/1997 per ogni organismo di telecomunicazione, di rendere disponibili gli elenchi degli abbonati e degli utenti al C.e.d. del Ministero dell'interno: cfr. *Relazione per l'anno 1997*, cap. 4.8, pagg. 87 e ss.).

L'emanazione di un apposito decreto legislativo al fine di adeguare la normativa di settore ai criteri direttivi e ai principi della normativa comunitaria e della raccomandazione del Consiglio d'Europa (95) 4 del 7 febbraio 1995 era stata prevista dalla legge delega n. 676/1996 (art. 1, comma 1, lett. *b*), n. 7).

Una disciplina più specifica in proposito è stata introdotta poi dalla direttiva n. 97/66/CE del Parlamento europeo e del Consiglio «sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni».

Il d.lg. n. 171/1998 ha dato pertanto attuazione a tali disposizioni comunitarie nel quadro dei principi generali contenuti nelle leggi nn. 675/1996 e 676/1996, tenendo conto delle norme delineate dal menzionato d.P.R. n. 318/1997 e dal d.m. 25 novembre 1997 sul rilascio delle licenze individuali, che avevano anticipato già il recepimento nell'ordinamento italiano di un primo corpo di disposizioni comunitarie.

Vengono di seguito segnalate, sinteticamente, alcune disposizioni più significative introdotte dal citato decreto legislativo.

- **Definizioni** - L'art. 1 propone le definizioni tecniche di abbonato, utente ecc. e, in un sistema ormai aperto alla concorrenza fra diversi operatori, fissa la distinzione fra «rete pubblica di telecomunicazioni» e «servizio di telecomunicazioni», consistente quest'ultimo «nella trasmissione e nell'instradamento di segnali su reti di telecomunicazioni, ivi compreso qualsiasi servizio interattivo anche se relativo a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi» (art. 1, comma 1 lett. d)).

- **Sicurezza e riservatezza delle comunicazioni** - Particolare attenzione è prestata a questi profili con obblighi che rimandano alle prescrizioni dell'art. 15 della l. n. 675/1996 e che impongono un onere di informativa da parte dei fornitori dei servizi di telecomunicazione nei confronti degli abbonati, specie quando sussistano particolari rischi di violazione della sicurezza della rete.

I fornitori di servizi devono informare, altresì, abbonati e utenti circa la «sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti a esse estranei» (art. 3, comma 1).

Analogo obbligo di informativa grava sull'abbonato quando i terminali o comunque le apparecchiature utilizzate possano determinare il rischio che il contenuto delle conversazioni fatte dall'utente sia appreso da estranei (art. 3, comma 2). Va ricordato poi l'obbligo dell'utente di avvisare le persone con le quali conversa, qualora faccia uso del meccanismo cd. «viva voce» (art. 3, comma 3).

Dati relativi a traffico, modalità di pagamento, fatturazione dettagliata - Il decreto definisce con precisione quali dati personali (indirizzo, numero dell'abbonato, numero totale degli scatti nel periodo ecc.) possono essere utilizzati per le esigenze di fatturazione, essendo invece obbligatorio cancellare o rendere anonimo al termine della chiamata ogni altro dato personale eventualmente memorizzato. Tale trattamento a fini di fatturazione è consentito, peraltro, «sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento» (art. 4, comma 2).

Allo scopo di garantire maggiormente la tutela della riservatezza degli utenti la normativa impone ai fornitori dei servizi di adottare anche modalità di pagamento alternative alla tradizionale fatturazione, tali da permettere di utilizzare il terminale con altra modalità di pagamento anche anonimo (ad esempio carte di credito, carte telefoniche prepagate ecc.).

Per quanto concerne l'invio della fattura ordinaria, il d.lg. n. 171 prevede invece il diritto di ricevere, gratuitamente e dietro richiesta, l'indicazione dettagliata degli elementi dimostrativi degli oneri addebitati. Però, se ci si avvale di questo servizio, a garanzia soprattutto della riservatezza dei diversi utenti, devono essere mascherate le ultime 3 cifre del numero chiamato. Quest'ultima prescrizione ha tenuto presenti sia le indicazioni provenienti dal confronto in ambito europeo, sia il rapporto fra cifre mascherate e lunghezza totale dei numeri delle utenze telefoniche.

- **Identificazione della linea, chiamate di disturbo e indesiderate** - Le nuove tecnologie digitali, che permettono l'identificazione immediata sugli apparecchi telefonici della linea chiamante, hanno imposto l'adozione di apposite misure di sicurezza.

Al riguardo, l'art. 6 prevede le diverse ipotesi che permettono agli abbonati e agli utenti di essere informati su tali servizi e di impedire, a seconda dei casi, l'identificazione della linea chiamante o di quella chiamata.

L'art. 7 prevede invece una procedura agevole per permettere di superare la soppressione dell'identificazione della linea chiamante e, nel contempo, di conoscere i dati relativi alla provenienza della chiamata ricevuta, qualora un abbonato si trovi nella condizione di ricevere chiamate di disturbo.

È previsto poi che le chiamate a scopo pubblicitario o per il compimento di ricerche di mercato o di comunicazione commerciale interattiva siano possibili solo con il consenso espresso dell'abbonato, qualora avvengano con l'utilizzo del telefax o mediante un sistema automatizzato di chiamata.

Ulteriori garanzie sono apprestate poi per permettere a ogni abbonato di poter bloccare il trasferimento automatico, verso la propria linea, di chiamate effettuate da parte di terzi (art. 8).

L'art. 10 prevede, invece, alcuni diritti aggiuntivi dell'abbonato in ordine alla compilazione degli elenchi telefonici. In particolare l'abbonato, «gratuitamente e con richiesta documentata per iscritto, ha diritto di non essere incluso negli elenchi, di ottenere che il suo indirizzo sia in parte omesso e, se ciò è fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso».

2.12.1.2 Prime esperienze applicative

Con l'entrata in vigore di questa nuova disciplina sono emersi però alcuni problemi in ordine alla sua corretta applicazione e il Garante è intervenuto per fornire alcuni primi chiarimenti di carattere generale.

Una questione è stata posta in relazione al termine per la conservazione dei dati relativi al traffico telefonico da parte dei gestori dei servizi di telecomunicazione.

Al riguardo, il Garante ha fatto presente che il d.lg. n. 171/1998 ha fissato un termine che in precedenza era imprecisato. Il decreto ha infatti previsto che i dati possano essere trattati e conservati dal fornitore del servizio telefonico «sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento» (v. l'art. 4, comma 2). Tale termine impone un riferimento all'art. 2948 del c.c. ed è, quindi, di cinque anni.

L'Autorità ha inoltre chiarito che entro il medesimo termine l'autorità giudiziaria può certamente acquisire dati in conformità alla legge, per finalità di indagine, proprio come è avvenuto per gravi fatti di criminalità, senza che sia necessario cancellarli una volta acquisiti agli atti d'indagine.

Il Garante ha affrontato poi la questione relativa alla mancata indicazione da parte dei fornitori dei servizi telefonici delle ultime tre cifre delle utenze telefoniche chiamate nella fatturazione dettagliata richiesta dagli abbonati. Diversi cittadini, liberi professionisti, imprenditori, associazioni, enti e altri organismi (pubblici e privati) abbonati al servizio telefonico hanno lamentato che tale misura non permette loro di verificare l'esattezza delle chiamate addebitate nella bolletta.

A seguito delle numerose segnalazioni ricevute, l'Autorità ha deciso di fornire alcuni chiarimenti, segnalando ai gestori del servizio telefonico alcuni opportuni aggiustamenti, con un provvedimento adottato il 5 ottobre 1998.

Nel provvedimento si è confermata la legittimità della misura del «mascheramento» di alcune cifre delle utenze chiamate, introdotta, come già detto, dal d.lg. n. 171 e praticata da tempo in diversi Paesi europei (anche prima dell'adozione della direttiva comunitaria, con l'oscuramento di un numero di cifre da due a quattro: Austria, Danimarca, Finlandia, Francia, Germania e Lussemburgo). Al

tempo stesso, si è però evidenziato che il «mascheramento» non permette di controllare a fondo l'esattezza di alcuni addebiti e può essere quindi «superato» qualora l'abbonato contesti la bolletta ricevuta e abbia l'esigenza di identificare puntualmente le chiamate effettuate, intendendo tutelare i propri diritti in sede giudiziaria.

Dal punto di vista normativo, sia la direttiva comunitaria, sia il d.lg. n. 171/1998 non mettono in discussione il diritto dell'abbonato di controllare l'esattezza degli addebiti e ne ampliano anzi la tutela, ma cercano di conciliare questo diritto con i diritti di altri soggetti la cui sfera privata è coinvolta anch'essa dalla fatturazione dettagliata: ossia di coloro che effettuano chiamate attraverso gli apparecchi collegati alla stessa linea telefonica (ad esempio, nel caso di utenze domestiche, i vari componenti del nucleo familiare o, nell'ipotesi di un'azienda, i dipendenti e i collaboratori), sia, altresì, dei destinatari delle telefonate (abbonati chiamati).

La l. n. 675/1996 non ostacola l'esercizio dei diritti degli abbonati e permette ai fornitori dei servizi telefonici di comunicare all'abbonato anche le cifre «mascherate» nella fattura in caso di contestazioni riguardanti l'esattezza di determinate chiamate addebitate all'abbonato medesimo, che quest'ultimo possa far valere con un'azione legale.

Qualora, quindi, le verifiche effettuate sulla base delle informazioni già riportate nella fattura dettagliata (che, intrecciate tra di loro, permettono già di riscontrare un congruo numero di situazioni, nonostante le cifre «mascherate») non siano sufficienti a fugare eventuali dubbi sull'effettuazione di determinate chiamate, o addirittura inducano a ritenere sicuramente erroneo l'addebito (ad esempio, nell'ipotesi di temporanea assenza del nucleo familiare dalla propria abitazione), l'abbonato può sollecitare un'attenta verifica dei numeri telefonici oggetto di contestazione.

Concretamente, l'abbonato può rivolgersi al gestore telefonico, senza particolari formalità e con una procedura snella, contestando la circostanza che determinate telefonate siano state effettuate dai propri apparecchi; il gestore deve verificare le chiamate «contestate», comunicando all'abbonato se l'addebito, dopo il controllo, resta fondato. Laddove tale riscontro non giunga, o comunque permanga un giustificato e motivato dubbio nell'abbonato, quest'ultimo ha diritto di chiedere e di ottenere gratuitamente dal gestore la comunicazione per intero dei numeri telefonici oggetto di precisa contestazione.

Il Garante ha quindi ritenuto che, in questi limiti, la comunicazione di determinati dati invece «mascherati» nella fattura dettagliata sia pienamente compatibile con i principi sanciti dalla l. n. 675/1996, la quale rende ammissibile per il titolare del trattamento (nel caso di specie, il gestore telefonico) la comunicazione dei dati personali, quando tale operazione risulti necessaria per far valere o difendere un proprio diritto in sede giudiziaria (art. 20, comma 1, lett. g)).

L'Autorità ha però aggiunto che le nuove tecnologie permettono oggi di bilanciare in maniera più efficace i diritti dell'abbonato con la *privacy* degli utenti e degli altri abbonati. La direttiva 97/66/CE e il d.lg. 171 prevedono infatti la possibilità di ricorrere a misure alternative al «mascheramento».

In particolare, secondo la direttiva, tali misure possono consistere nell'introduzione di possibilità di pagamento «che permettano un accesso anonimo, o rigorosamente privato, ai servizi di telecomunicazione offerti al pubblico, quali carte telefoniche, oppure possibilità di pagamento con carta di credito» (considerando 18 della direttiva 97/66/CE). In tal modo, sia dalle utenze private sia dai luoghi di lavoro, la persona chiamante - che non sempre corrisponde all'abbonato pagante - potrebbe fare un legittimo uso dell'utenza senza far gravare il costo delle chiamate sull'abbonato; tali chiamate, quindi, non sarebbero riportate nel dettaglio di fatturazione. Anche il decreto ha fatto un passo significativo introducendo, appunto, l'obbligo

per i gestori di consentire «che i servizi richiesti e le chiamate effettuate da qualsiasi terminale possano essere pagate con modalità alternative alla fatturazione, anche anonime, quali le carte di pagamento o prepagate» e che, in questo caso, tali servizi e chiamate non debbano comparire nella fatturazione (art. 5, commi 1 e 2).

Sotto questo aspetto, il Garante ha perciò raccomandato ai fornitori dei servizi di telefonia la necessità di dare rapida attuazione al d.lg. n. 171/1998, rendendo effettiva e agevole la possibilità per gli abbonati e gli utenti di avvalersi, in alternativa alla fatturazione dettagliata, di strumenti di pagamento delle chiamate telefoniche che garantiscano l'anonimato.

In relazione invece alle modalità e ai limiti della procedura concernente la contestazione delle fatture telefoniche e la «messa in chiaro» dei numeri relativi alle telefonate «controverse», l'Autorità ha trasmesso il proprio provvedimento, adottato il 5 ottobre 1998, alle competenti amministrazioni, al fine dell'eventuale aggiornamento, alla luce delle nuove disposizioni del d.lg. n. 171, delle norme regolamentari sulle condizioni di abbonamento al servizio telefonico e di eventuali altre disposizioni in materia.

Successivamente è stata avviata un'indagine per verificare il rispetto da parte delle società che gestiscono il servizio telefonico dei principi indicati nel predetto provvedimento. Infatti, da segnalazioni pervenute all'Ufficio è emerso che alcuni gestori non avevano adempiuto alle richieste di utenti volte a conoscere nel dettaglio tutte le cifre delle chiamate contestate. Dall'indagine, tuttora in corso, si è potuto appurare che le aziende che forniscono i servizi telefonici intendono senz'altro aderire alle indicazioni fornite dal Garante, ma adducono la necessità di disporre di tre o quattro mesi per il pieno adeguamento dei servizi.

Alcuni chiarimenti sono stati infine forniti dal Garante con riferimento alla possibilità per i competenti ispettorati del Ministero delle comunicazioni di accedere, presso una società che gestisce il servizio di telefonia mobile, ad alcuni documenti contenenti dati relativi ad abbonati e utenti, presi a campione, al fine di verificare la regolare osservanza degli obblighi assunti dal concessionario e la regolarità del servizio.

Al riguardo, l'Autorità ha sottolineato che vi è una complessa serie di norme che hanno attribuito al Ministero ampi poteri di vigilanza e di controllo sull'operato delle società concessionarie dei servizi telefonici (in particolare, quelle che prevedono la disciplina convenzionale del rapporto di concessione), e che la l. n. 675/1996 non ostacola la comunicazione di dati personali al Ministero medesimo. Spetta però a quest'ultimo, da un lato individuare le disposizioni in presenza delle quali è possibile acquisire i dati anche senza che il privato gestore del servizio telefonico raccolga il consenso degli abbonati interessati e, dall'altro, valutare caso per caso la possibilità di svolgere con pari efficacia i compiti a esso affidati anche sulla base, in tutto o in parte, di informazioni anonime.

È stata infine segnalata al gestore l'esigenza che le informative inviate agli abbonati rechino, ove già non previsto, un generale riferimento alle comunicazioni dei loro dati obbligatorie per legge o regolamento.

2.12.2 Video-sorveglianza

L'Italia manca tuttora di una normativa che disciplini specificamente la video-sorveglianza, a differenza di quanto avviene in altri Paesi europei come la Francia, la Danimarca, l'Islanda e la Norvegia. La direttiva comunitaria n. 95/46/CE del 1995 e la convenzione n. 108/1981 del Consiglio d'Europa applicano in modo vincolante la disciplina del trattamento dei dati personali anche ai suoni e alle immagini

(quali sono quelli registrati nei controlli video) nel caso consentano l'identificazione di un soggetto anche in via indiretta (ad es. mediante collegamento con altre informazioni).

La l. 31 dicembre 1996, n. 675 che ha attuato la convenzione n. 108 e ha recepito la direttiva europea, considera come «dato personale» qualunque informazione che consenta l'identificazione dei soggetti interessati sebbene derivante da suoni e da immagini anziché da dati alfanumerici. Tale legge è quindi senz'altro applicabile ai trattamenti di suoni e di immagini effettuati attraverso sistemi di video-sorveglianza. Anche in caso di non chiara e univoca identificazione dei soggetti inquadrati da telecamere (possono creare a ciò un ostacolo la distanza, l'ampiezza dell'angolo visuale, la qualità degli strumenti, ecc.), va ritenuta sufficiente la possibilità di identificazione attraverso l'interconnessione con documenti di archivio e banche dati di immagini in possesso di altre autorità quali quelle di polizia.

Nell'ambito della sua attività il Garante ha perciò sollecitato il rispetto di alcune specifiche prescrizioni della l. 31 dicembre 1996, n. 675.

In risposta, ad esempio, ai quesiti di alcuni comuni in ordine alla legittimità di taluni progetti relativi all'installazione di telecamere in luoghi pubblici (nella specie, in un parco e in zone deturpate con maggiore frequenza da atti di vandalismo), il Garante ha richiamato l'attenzione su taluni aspetti che devono essere tenuti presenti ogni qualvolta si prospetti l'esigenza di installare sistemi di video-sorveglianza:

a) verificare la legittimità e le finalità dell'iniziativa, controllando anche se la stessa corrisponda alle funzioni istituzionali demandate all'ente pubblico;

b) controllare l'idoneità delle misure che possono essere adottate per assicurare un uso corretto dei dati da parte dei soggetti legittimati (art. 15);

c) vigilare sulle modalità di registrazione iniziale dei dati e della loro conservazione, anche al fine di assicurare la loro pertinenza e non eccedenza rispetto agli scopi perseguiti (art. 9, comma 1, lettera d));

d) definire le procedure e le modalità volte a fornire agli interessati le informazioni previste (art. 10).

In questo quadro il Garante ha manifestato perplessità dinanzi alla prospettiva dell'attivazione di un sistema di video-sorveglianza privo di un insieme articolato di garanzie, che dovrebbero riguardare, in modo particolare, l'eventuale intenzione di conservare le immagini in un apposito archivio, l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'ente e l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici.

Fornendo riscontro a una richiesta di parere in ordine alla compatibilità con la l. 31 dicembre 1996, n. 675 del progetto di installazione di apparecchiature di video-sorveglianza presso il pronto soccorso di una azienda ospedaliera, il Garante ha sottolineato come i dati personali che rilevavano nel caso in specie fossero in massima parte dati sensibili, poiché le telecamere da installare riprendevano essenzialmente immagini di persone ammalate.

Il trattamento di dati sensibili da parte di un'azienda ospedaliera è apparso connesso all'assistenza e alla cura dei pazienti ricoverati che rientrano nelle finalità istituzionali proprie degli organismi sanitari pubblici.

Tale generale compito di assistenza, infatti, si specificava in un'attenzione continua ai ricoverati in rianimazione e in un doveroso controllo di sicurezza all'interno del pronto soccorso. Si trattava, quindi, di operazioni condotte da sempre con modalità tradizionali, che verranno ora svolte con l'ausilio di sistemi di video-sorveglianza. Il combinato disposto degli artt. 22, comma 3 e 41, comma 5 della l. n. 675/1996 ha legittimato quindi l'azienda ospedaliera a installare le telecamere e a trattare i relativi dati sensibili. Peraltro, l'installazione del sistema di video-sorve-

glianza ha richiesto che fossero osservate alcune prescrizioni poste dalla l. n. 675/1996. Prima di attivare le apparecchiature di ripresa, la direzione dell'azienda ospedaliera dovrà infatti opportunamente regolamentare i seguenti profili:

a) determinare con precisione la localizzazione delle telecamere e le modalità di ripresa, in aderenza alle finalità che hanno suggerito l'installazione del sistema di video-sorveglianza e nel rispetto dei principi fondamentali fissati dall'art. 9 della legge, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

b) definire puntualmente i soggetti legittimati a trattare i dati personali in oggetto, individuando eventualmente un soggetto responsabile, ai sensi dell'art. 8 della legge, del sistema di video-sorveglianza nonché gli incaricati del trattamento (personale infermieristico, addetti alla vigilanza, ecc.);

c) stabilire idonee misure di sicurezza ai sensi dell'art. 15 della legge, al fine di assicurare un corretto uso dei dati, evitando il rischio che gli stessi possano entrare nella disponibilità di persone estranee alla struttura o comunque non autorizzate. Si è sollecitata pertanto una particolare attenzione alle modalità di accesso alle riprese video da parte dei familiari dei ricoverati in rianimazione, ai quali andrà consentita, nella misura tecnicamente possibile, la visione delle sole immagini del loro congiunto;

d) fissare parametri precisi per quanto riguarda l'eventuale necessità di conservazione delle immagini registrate, secondo il dettato dell'art. 9, comma 1, lettera e) della legge che prescrive la conservazione dei dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

e) prevedere forme e modalità volte a fornire agli interessati le informazioni previste dall'art. 10 della legge.

Si segnala infine che il Garante segue con attenzione l'attività del Comitato di sorveglianza del programma operativo «Sicurezza per lo sviluppo del Mezzogiorno d'Italia». Nel programma riveste una importanza particolare il progetto relativo al rafforzamento della sicurezza sull'asse autostradale Caserta-Salerno-Reggio Calabria, che prevede l'utilizzo di moderne tecnologie video e audio per il controllo del territorio.

Considerata anche la vastità del territorio oggetto del controllo, è apparso necessario acquisire maggiori elementi sulle finalità di tale sistema di controllo e sulla sua base normativa, per verificare se i trattamenti in questione rientrano fra quelli indicati dall'art. 4 della legge, oppure siano ricompresi tra quelli ai quali la legge si applica senza eccezioni. Il Garante ha chiesto quindi notizie più dettagliate circa:

a) la modalità con la quale verranno gestite le immagini riprese (memorizzazione, conservazione, angolo visuale delle telecamere e limite della possibilità di avvicinamento dell'immagine);

b) le modalità con le quali verranno effettuate eventuali rilevazioni di tipo acustico, appurando, in particolare, se esse si sostanzino in un controllo fonico di ciò che si svolge all'interno delle aree di servizio ovvero si limitino al raggio di azione delle telecamere, e quale sia inoltre il livello di percezione dei suoni;

c) i meccanismi che si intendono predisporre per fornire un'adeguata informazione agli interessati;

d) le misure di sicurezza adottate, considerato che le immagini saranno trasmesse dalle telecamere ai centri operativi attraverso il sistema di comunicazione satellitare.

Il Ministero dell'interno ha già fornito le notizie richieste e gli approfondimenti in atto sono in via di definizione.

Allo scopo di avere un quadro dettagliato e capillare del fenomeno, il Garante ha deciso infine di affidare una ricerca sulle diverse forme di video-sorveglianza utilizzate sempre più intensivamente a scopi di sicurezza sociale in luoghi pubblici, esercizi commerciali, supermercati, banche, ecc. La decisione è stata presa in attesa della complessiva regolamentazione della materia attraverso uno dei decreti che il Governo è stato delegato a emanare (in base all'art. 1, comma 1, lettera i) della l. n. 676/1996) e che dovrà fissare le norme per il giusto equilibrio tra il diritto alla riservatezza dei cittadini e le esigenze di pubblica sicurezza e della prevenzione dei reati. La non procrastinabilità di una normativa in materia di video-sorveglianza è peraltro implicitamente evidenziata dal fatto che l'art. 11 della l. n. 449/1997 («collegato» alla finanziaria 1998) prevede per le aziende commerciali e turistiche la possibilità di beneficiare di crediti d'imposta per l'acquisto di sistemi di sicurezza, incluse le telecamere a circuito chiuso.

È da segnalare, peraltro, che se in Italia l'installazione di telecamere in funzione di deterrenza anticrimine o di accertamento di violazioni al codice della strada è stata all'ordine del giorno in varie occasioni, il 1998, all'estero, ha segnato un vero e proprio salto di qualità.

L'efficacia raggiunta dai sistemi elettronici di controllo alimenta paure talvolta irrazionali, ma è anche vero che nella società contemporanea l'equilibrio tra libertà e sicurezza tende a essere risolto, in proposito, trascurando i diritti di libertà.

Alcuni episodi indicati qui a titolo meramente esemplificativo possono risultare utili.

Nel mese di ottobre il comune di Newham (Londra) ha avviato un piano di modernizzazione della rete già esistente di 140 telecamere fisse e 11 mobili. L'intero apparato di video-sorveglianza è stato dotato di un sistema elettronico di riconoscimento visuale collegato a un archivio biometrico: il software, denominato «*Mandrake*», è all'avanguardia nei sistemi di scannerizzazione e si basa su algoritmi di reti neurali (i sistemi di apprendimento sviluppati nel settore dell'intelligenza artificiale). Quando un soggetto entra nel campo visivo della telecamera, il fotogramma del viso viene isolato da un cerchio rosso ed esaminato dal computer. Se il computer riconosce l'immagine nella banca dati suona l'allarme e la polizia (che collega all'introduzione del circuito di controllo video una diminuzione significativa dei reati) viene allertata su una linea speciale.

Sistemi analoghi sono in uso al confine tra USA e Messico (al riguardo si è parlato della costruzione di una nuova «Cortina di silicio» dopo il crollo della «Cortina di ferro» in Europa) e vengono sperimentati negli aeroporti. La novità è costituita dalla potenza del software: «*Mandrake*» è in grado infatti di scannerizzare più visi contemporaneamente, a differenza di altri prodotti informatici in grado di analizzare l'identità di una sola persona per volta.

Al perfezionamento tecnologico degli apparati di sorveglianza corrisponde però una mobilitazione delle associazioni per la difesa dei diritti civili. A New York la NYCLU (affiliata della ACLU, l'American Civil Liberties Union) ha organizzato un censimento delle telecamere funzionanti nelle strade di Manhattan. Nel mese di dicembre sono stati presentati alla stampa i risultati del lavoro: il NYC Surveillance Camera Project ha prodotto una mappa di 2397 telecamere (2117 private e 270 di organismi pubblici) distribuite in 12 zone. La mappa non ha la pretesa di essere esaustiva poiché molte telecamere sono mimetizzate, ma i risultati sono stati sufficienti a definire la grande metropoli statunitense «a surveillance camera town» (comunicato stampa della NYCLU del 13 dicembre 1998).

2.12.3 Commercio elettronico

Il commercio elettronico non rappresenta un fenomeno del tutto nuovo, poiché per molti anni le imprese si sono scambiate dati commerciali usando diverse reti di comunicazione. Dal momento in cui Internet ha iniziato il suo *trend* di maggiore sviluppo, oramai considerato esponenziale anche dagli osservatori più cauti, il commercio elettronico non è più limitato alle grandi aziende, ma si apre a chiunque nel mondo.

Internet somiglia sempre più a un'enorme e infinita fiera commerciale con innumerevoli servizi diffusi in tutto il mondo, accessibili attraverso il *World Wide Web* (WWW). Anche in Italia la crescita del commercio elettronico, soprattutto per quanto riguarda i rapporti fra imprese e consumatori, sarà superiore, a detta degli osservatori, alla crescita media del complessivo volume di affari. Oltre a creare nuove forme di attività, il commercio elettronico influirà profondamente sul modo di condurre gli affari e avrà forti ripercussioni sulla sfera della vita privata degli utenti delle reti e dei consumatori. Di qui l'esigenza di un approccio attento ai diritti della personalità e, al tempo stesso, ben modulato, in modo da non pregiudicare l'uso della telematica per facilitare acquisti e relazioni commerciali via Internet.

Si moltiplicano, al riguardo, le iniziative di riflessione dalle quali emergono, giorno dopo giorno, nuovi temi da approfondire (correttezza e trasparenza delle relazioni con l'utente; consapevolezza da parte dell'utente degli effetti dei suoi comportamenti in rete; presenza ed efficacia di informazioni sintetiche, ma irrinunciabili da fornire agli utenti; distinzione dei trattamenti di dati legati al rapporto commerciale da quelli effettuati per marketing, ricerche di mercato e studi su utenti; sicurezza delle transazioni; diritto all'anonimato).

La delicatezza delle scelte da effettuare emerge anche dalla complessità delle relazioni che si intrecciano a margine delle transazioni elettroniche. Il numero dei soggetti partecipanti moltiplica poi il novero dei trattamenti, alcuni dei quali non vengono individuati in quanto tali dall'utente, ovvero dal *cliente*.

Oltre ai due soggetti più direttamente interessati alla transazione commerciale elettronica, il cliente e il venditore - quest'ultimo nel senso più ampio del termine, che può indicare anche un'amministrazione o un sito *Web* che fornisca informazioni o pubblicità senza concludere una transazione commerciale - occorre infatti identificare anche altri soggetti interessati anch'essi, in qualche modo, dal negozio elettronico. Ci si riferisce, in particolare :

- al *fornitore di accesso Internet* (*Internet access provider*), che fornisce agli utenti l'infrastruttura tecnica di rete necessaria per accedere a Internet;
- al *vettore*, ossia all'organismo di telecomunicazioni che fornisce la rete di base per il trasferimento dei dati;
- al *fornitore di servizio Internet* (*Internet service provider*), che fornisce servizi per la memorizzazione, la trasmissione e la presentazione dei contenuti;
- ai *siti Web* che offrono *motori di ricerca*, sempre più diffusi data l'enorme mole di informazioni disponibile in Rete. Questi siti comportano un duplice rischio: da un lato hanno la possibilità di raccogliere dati su un determinato individuo ricavandoli da più siti, potendone così ricavare un profilo di personalità; in secondo luogo, i fornitori di questi motori di ricerca possono elaborare un profilo dettagliato degli interessi manifestati dai propri utenti;
- alle *banche e/o alle istituzioni finanziarie*, che intervengono nelle transazioni commerciali elettroniche.

Uno stesso soggetto può infine offrire servizi diversi in ambiente Internet, direttamente o attraverso soggetti controllati. Ne deriva che sarà difficile individuare i legami e i flussi esistenti fra soggetti che appartengono a uno stesso consorzio/gruppo e fra le funzioni esercitate da uno stesso soggetto.

Da questo quadro sintetico appare chiaro che una delle prime esigenze che si pone è quella di creare per gli utenti un clima di fiducia e di sicurezza circa la liceità, la trasparenza e la correttezza del trattamento dei dati personali nel commercio elettronico. A tale scopo è necessaria una strategia integrata che deve saper coniugare nel loro giusto ruolo un nocciolo «duro» di regole normative con altre norme nascenti «dal basso» attraverso efficaci codici di deontologia e di buona condotta, tecnologie pulite in grado di selezionare l'uso di dati personali specie per piccoli acquisti effettuabili su base anonima, ed eventuali meccanismi di classificazione di siti in base alle garanzie offerte agli utenti, basati su criteri obiettivi e accettati di certificazione.

In altre parole, l'impiego diffuso delle nuove tecnologie dell'informazione e della comunicazione, che rappresenta la caratteristica primaria del commercio elettronico, induce a pensare all'eventualità di un approccio diverso rispetto alla realizzazione dei più comuni strumenti normativi.

Viene soprattutto in rilievo il dato strutturale della rete transnazionale, secondo il quale la diffusione e la circolazione delle informazioni a livello planetario comportano sia una minore possibilità di controllo dei percorsi seguiti (quindi un maggiore rischio di intrusione nella vita privata degli individui che accedono alla rete), sia un problema di individuazione della normativa di tutela di volta in volta applicabile secondo le diverse aree geografiche. Infatti l'organizzazione e gli effetti delle informazioni e dei dati in transito su reti aperte coinvolgono tre livelli: la disciplina internazionale, quella comunitaria e quella degli ordinamenti interni. Tali caratteristiche mettono in luce come i rischi di violazione della riservatezza siano tutt'altro che remoti.

A nuovi rischi devono perciò corrispondere nuovi principi e nuovi concetti, al fine di assicurare nei modi opportuni la tutela dei dati di ciascun soggetto.

Lo stesso Consiglio di Stato francese, in un suo documento su Internet e le reti numeriche (2 luglio 1998), evidenzia come «le reti numeriche transfrontaliere inducono una modificazione sostanziale dei modi di regolazione abituale dei sistemi giuridici. Da una parte la regolamentazione di origine statale deve ormai combinarsi con l'autoregolazione dei protagonisti, degli attori, dei servizi comunicativi; d'altra parte, tenuto conto dei limiti inerenti a ogni iniziativa puramente nazionale, spetta alla cooperazione internazionale fra gli Stati far rispettare gli interessi pubblici in uno spazio largamente dominato dall'iniziativa privata. In altri termini, le reti introducono una doppia interdipendenza, tra attori pubblici e privati nell'ambito degli Stati medesimi».

La rapidità dello sviluppo tecnologico da una parte, e l'inevitabile lentezza del processo legislativo dall'altra, rischiano di rendere rapidamente obsoleto un impianto normativo teso a regolamentare in maniera «classica» l'ambiente Internet e le applicazioni che esso consente, fra cui il commercio elettronico.

Non a caso alcune esperienze come quella olandese, ruotano attorno a una normativa a tempo «determinato». La stessa recente legge tedesca (Legge sulla informazione e la comunicazione - IUK Dg 13-6-97, art. 2 (4)) sceglie di individuare e fissare quattro principi di tipo generale, idonei ad adattarsi all'innovazione tecnologica.

Il primo è quello della «minimizzazione dei dati» (il titolare deve sottoporre a trattamento il minimo di dati necessario per assicurare il corretto svolgimento del trattamento stesso).

Il secondo è il diritto all'anonimato (riconosciuto anche in altri contesti come quello della firma elettronica; collegato a esso il diritto a utilizzare uno pseudonimo).

Il terzo riguarda la cd. «integrazione delle funzionalità tecnologiche» al fine di dare attuazione ai principi di protezione dei dati (esso implica che ogniquale volta le tecnologie utilizzate per la raccolta o il trattamento dei dati possano essere considerate anche uno strumento per attuare o potenziare i principi di protezione dei dati, queste stesse tecnologie debbono essere configurate in modo conforme a tale principio).

Il quarto principio è quello della «realizzazione elettronica dello *status* giuridico dell'interessato» (il che comporta la necessità di garantire la trasparenza e la realizzazione, attraverso tecniche on-line, dei vari diritti degli utenti *Web*, anche attraverso l'intervento tempestivo delle autorità nazionali incaricate della protezione dei dati).

Le innumerevoli possibilità tecniche offerte dalle reti aperte del sistema comunicativo mettono però a dura prova le tradizionali strutture giuridiche in numerosi contesti, riguardanti soprattutto la protezione dei diritti fondamentali della persona. Sorge perciò l'impegno per i molteplici organismi regolatori, sia di diritto interno sia di diritto internazionale, di comporre il quadro delle regole. Di qui la necessità, largamente condivisa a livello comunitario, che le attività condotte su Internet non possano essere svincolate dai principi giuridici fondamentali che valgono *off-line* o per altri settori. E se da un lato bisogna accordare piena tutela ai diritti fondamentali, dall'altro anche nel cd. *cyberspazio* deve valere la regola che ogni eventuale limitazione dei diritti e delle libertà fondamentali deve essere adeguatamente giustificata, necessaria e proporzionata anche alla luce delle garanzie previste dalla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali.

Circa la posizione italiana, il nostro Paese, in coerenza con gli orientamenti delle istituzioni europee e in particolare con gli enunciati della Conferenza europea del luglio 1997 a Bonn, ravvisa l'esigenza di costruire una normativa adeguata a un duplice livello, di cui il primo nel quadro delle fonti sovranazionali (v. anche § 4.2.3 per quanto riguarda la proposta di direttiva sul commercio elettronico) e il secondo nell'ambito del diritto nazionale.

E se preminente è la via dell'intervento normativo, non è però da trascurare la prospettiva di una valorizzazione più ampia dei codici di autodisciplina, in quanto il policentrismo delle fonti di regolazione, purché dotate di concreta efficacia, può svolgere anche qui un importante ruolo integrativo. In tal senso va ricordato nuovamente come la l. 31 dicembre 1996, n. 675, preveda esplicitamente tali codici e riconosca loro questa funzione: non tanto, quindi, una rinuncia a legiferare, quanto piuttosto il tentativo di sperimentare modi e sedi di produzione di regole più vicini alla realtà da disciplinare e perciò, forse, più efficaci.

Va ricordato che di recente il nostro legislatore, recependo la direttiva n. 97/66/CE, ha emanato il d.lg. 13 maggio 1998, n. 171, recante disposizioni di tutela della vita privata nel settore delle telecomunicazioni (v. § 2.12.1). Il Governo sarà inoltre impegnato a dare attuazione alla delega prevista dalla l. 31 dicembre 1996, n. 676, che all'art. 1, comma 1, lett. n) prevede di «stabilire le modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti ai servizi accessibili al pubblico e la corrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale».

La fiducia del cittadino rappresenta sicuramente un elemento chiave per lo sviluppo del commercio elettronico (rilevante per lo sviluppo del sistema economico del Paese) e il pieno rispetto del diritto alla riservatezza e all'identità personale ne costituisce una componente essenziale.

Strettamente connesse al tema sono anche la certezza delle transazioni, garantite da organismi di categoria (infrastrutture bancarie per la componente moneta elettronica e infrastrutture delle imprese o del commercio o dei servizi pubblici e privati per la componente qualità e fedeltà dei servizi e prodotti offerti), la sicurezza contro ogni violazione concernente le informazioni protette o gli strumenti di pagamento, nonché la sobrietà e selettività nel trattamento dei dati personali da parte degli erogatori di servizi.

Va sottolineata poi l'importanza delle tecnologie che garantiscono strumenti sicuri di pagamento elettronico. Per la tutela della riservatezza è necessario esaminare la possibilità che i pagamenti via Internet, per l'acquisto di determinati beni e per le cd. «piccole spese», siano effettuati in modo anonimo (vale a dire senza registrare l'identità di chi ha effettuato il pagamento) e sviluppare sistemi di pagamento elettronico con carte prepagate.

Infine, un *vademecum* esplicativo dei rischi per la riservatezza degli utenti, dei diritti degli utenti *Web* e degli obblighi in materia di protezione dei dati personali che incombono al titolare di un sito nel quale possono essere effettuate transazioni commerciali dovrebbe ricevere la massima diffusione mediante la rete Internet. L'Autorità di protezione dei dati sarà presto presente con un proprio sito *Web* documentato e aggiornato al fine di poter esercitare, anche in questo ambito, i propri fini istituzionali.

2.13 FLUSSI TRANSFRONTALIERI DI DATI

2.13.1 Profili generali

Con l'approvazione della direttiva comunitaria 95/46 CE, il cui termine per il recepimento è scaduto il 24 ottobre scorso, l'Unione europea ha introdotto un quadro di riferimento comune per la protezione dei dati personali destinato a tutti gli Stati membri, in modo da determinare discipline convergenti e omogenee e impedire, così, che situazioni di scarsa protezione in taluni contesti nazionali possano indurre altri Stati a restringere o vietare il flusso e la circolazione dei dati.

Come è noto tale normativa comunitaria è stata recepita in buona parte nella l. 31 dicembre 1996, n. 675, all'art. 28. Da tale quadro discende una situazione che garantisce la circolazione delle informazioni all'interno dell'Unione europea e la possibilità di esportare dati verso quei Paesi terzi che assicurino un livello di protezione «adeguato», anche se non necessariamente equivalente.

Il requisito dell'adeguatezza costituisce il fulcro del dibattito in atto a livello internazionale sul trasferimento dei dati all'estero.

Il meccanismo di valutazione dell'«adeguatezza», infatti, è complesso ed è disciplinato agli artt. 25 e 26 della direttiva, che attribuiscono il giudizio, in primo luogo, alle autorità di garanzia nazionali che cooperano attivamente tra loro, nonché ai giudici nazionali che siano eventualmente investiti del caso.

L'adeguatezza può essere però accertata anche su scala europea, procedendo a una valutazione comune (effettuata dalla Commissione in collaborazione con il Comitato previsto dall'art. 31 della direttiva) di uno o più settori o attività presenti in un Paese terzo, previa analisi della natura dei dati, delle finalità del trattamento e delle norme generali o settoriali vigenti.

L'art. 26 impone poi allo Stato membro sia di informare la Commissione e gli altri Stati aderenti circa le autorizzazioni in deroga al trasferimento concesse nei singoli casi, sia di uniformarsi alle decisioni che la Commissione riterrà opportuno assumere.

Per tale ultimo aspetto si avverte l'esigenza di creare un modello procedimentale comune, attraverso cui gli Stati membri possano pervenire a conformarsi alle decisioni demandate alla Commissione, come già indicato nella *Relazione per l'anno 1997* presentata al Parlamento da questa Autorità.

È bene ricordare, peraltro, che sono previste alcune situazioni nelle quali, pur non essendo gli Stati in grado di assicurare una protezione «adeguata», è però possibile trasferire comunque i dati, ricorrendo a talune garanzie considerate sufficienti. L'art. 26 della direttiva, attuato dall'art. 28, comma 4 della l. n. 675/1996, prefigura infatti alcune situazioni nelle quali può farsi a meno di applicare il principio di adeguatezza: così il trasferimento di dati in Paesi terzi è consentito qualora ricorrano determinati presupposti e condizioni, come ad esempio l'esistenza di un consenso dell'interessato, o di un'interesse pubblico rilevante, la conclusione o l'esecuzione di un contratto, la presenza di informazioni estraibili da elenchi pubblici o di una autorizzazione del Garante rilasciata a fronte di idonee garanzie prestate nei confronti degli interessati.

Si può, infine, supplire alla carenza del requisito dell'adeguatezza attraverso il ricorso a determinate clausole inserite in contratti, anche «tipo», da sottoporre all'esame delle singole Autorità nazionali oppure, se i contratti sono a livello europeo, della Commissione.

Benché i Paesi extracomunitari che garantiscono una tutela «adeguata» siano assai pochi, l'insieme di queste ulteriori previsioni, che introducono elementi e modalità sostitutivi, ha consentito che i flussi di dati in ambito pubblico e privato nel 1998 non subissero gravi restrizioni.

Tutti gli Stati membri e tutte le Autorità nazionali di controllo hanno dimostrato senso di responsabilità nel privilegiare soluzioni applicative non troppo rigide nell'attesa di un comune, primo, approccio europeo che potrà tener conto sia dei pareri espressi dal Gruppo previsto dall'art. 29 della direttiva, sia dell'esito dei lavori del Comitato di cui all'art. 31 della medesima direttiva (a cominciare dalle decisioni riguardanti alcuni Paesi terzi come Svizzera, Ungheria e Honk Kong, per finire al più complesso tema delle relazioni con gli USA). D'altra parte, è da tenere in debito conto che le garanzie adottate a protezione dei dati personali, se applicate solo da parte dei soggetti comunitari, porterebbero a una distorsione della concorrenza a favore di imprese extraeuropee su cui non gravano gli oneri derivanti dall'adozione di tali misure.

2.13.1.1 Alcuni casi applicativi

Sul versante interno, anche quest'anno sono pervenuti al Garante vari quesiti formulati da parte di titolari del trattamento, in ordine all'applicazione della disciplina sul trasferimento dei dati personali all'estero.

I chiarimenti richiesti riguardavano soprattutto l'obbligo di notificazione, i casi in cui questo può escludersi e la portata del principio di adeguatezza.

Nelle risposte l'Autorità ha richiamato le considerazioni e i criteri cui poco sopra si è fatto cenno, e ha confermato l'orientamento già espresso nel 1997, fornendo indicazioni tese a contribuire al processo di adeguamento in corso, anche per questi rilevanti profili, rispetto al nuovo sistema comunitario di protezione dei dati.

Il Garante si è pronunciato, poi, su un quesito presentato dalla Consob, chiedendo che la l. n. 675/1996 non ostacola il trasferimento di dati che la Commissione invia alle analoghe autorità di vigilanza degli altri Paesi in attuazione degli accordi internazionali.

L'art. 28, comma 4, lett. c) della legge, infatti, permette di trasferire comunque i dati all'estero, anche in Paesi extracomunitari, qualora il trasferimento sia necessario per salvaguardare un «interesse pubblico rilevante». Requisito rinvenibile, nel caso in specie, nella disciplina di settore (l. 17 maggio 1991, n. 157; d.lg. 23 luglio 1996, n. 415; d.lg. 24 febbraio 1998, n. 58).

Con l'occasione il Garante ha evidenziato che, grazie al differimento all'8 maggio 1999 dell'operatività della disposizione transitoria contenuta all'art. 41, comma 5, l. n. 675/1996 operato con il d.lg. n. 389, tale interpretazione è valida anche nel caso in cui il trasferimento riguardi dati di carattere giudiziario o «sensibile» (artt. 22, comma 3 e 24 della legge).

La Commissione e il Comitato di cui all'art. 31 della direttiva stanno portando avanti il dialogo con alcuni Paesi terzi e, in particolare, con gli USA. La consapevolezza della necessità di definire la questione a livello internazionale in tempi brevi ha acquistato maggiore concretezza proprio nell'ultimo anno, anche in considerazione della scadenza del termine di recepimento della direttiva europea.

In tale ottica il Garante, oltre a partecipare attivamente nelle sedi internazionali competenti, ha assunto l'iniziativa di organizzare, lo scorso mese di maggio a Roma, un convegno internazionale su «Internet e *privacy*» (v. anche § 3.2.5). Il tema è stato occasione per un confronto aperto e costruttivo tra le posizioni, e le culture stesse, prevalenti al riguardo negli Stati Uniti e in Europa e, tuttora, marcatamente distanti. In tal modo si è inteso fornire un contributo al dibattito e alla ricerca di una disciplina comune il più possibile uniforme in uno dei settori più vitali.

È da segnalare in questo quadro la stessa visita in Italia del Sottosegretario di Stato americano al commercio ambasciatore D.J. Aaron. Il 26 gennaio 1999, quest'ultimo si è recato presso l'Ufficio del Garante per esaminare con l'Autorità italiana i diversi punti di vista emersi a proposito della proposta americana di basare le garanzie per l'esportazione dei dati negli USA su un sistema di adesione volontaria delle imprese americane ad alcuni principi, osservati i quali, secondo gli USA, le imprese stesse potrebbero approdare a un *safe harbour*. La questione è ancora aperta in quanto il primo schema proposto dagli USA è stato considerato da vari Paesi europei e da tutte le Autorità nazionali europee di controllo meritevole di varie precisazioni e miglioramenti (v. il parere n. 1/1999 del Gruppo di cui all'art. 29 della direttiva, riportato negli allegati).

2.14 TRATTAMENTO DI DATI PER FINALITÀ DI GIUSTIZIA

Il trattamento di dati personali per ragioni di giustizia nell'ambito degli uffici giudiziari è soggetto solo ad alcune regole della l. n. 675/1996 (v. art. 4). Nell'attività del Garante, hanno avuto particolare rilievo sia l'individuazione dei limiti in cui la legge è applicabile, sia i principi di correttezza del trattamento, di pertinenza

e non eccedenza dei dati trattati, sanciti dall'art. 9 della legge anche in riferimento alla Convenzione n. 108/1981 del Consiglio d'Europa (e richiamati fra l'altro nella decisione del Garante del 22 ottobre 1998, relativa alla notificazione di atti giudiziari e amministrativi; v. § 2.1.7).

Tali principi non consentono, però, una disciplina sufficientemente dettagliata del trattamento di dati per finalità di giustizia, e al riguardo la l. n. 344/1998 ha prorogato al 31 luglio 1999 il termine per l'attuazione della delega al Governo a emanare disposizioni integrative contenuta nell'art. 1, comma 1, lett i) della l. n. 676/1996.

Possono essere ora ricordati alcuni casi significativi:

a) va ricordato, ad esempio, che in risposta ad alcuni quesiti formulati dalla Corte di appello militare di Roma, è stato fatto presente che la comune attività amministrativa relativa al personale di magistratura è assimilabile a quella di ogni altra amministrazione pubblica riguardante i propri dipendenti, facendo rinvio per ulteriori elementi alla deliberazione relativa al CSM adottata dal Garante il 2 dicembre 1997. È stata inoltre chiarita la perdurante applicabilità dell'art. 116 c.p.p., in base al quale, previa autorizzazione dell'autorità giudiziaria, chiunque abbia interesse può ottenere copie, estratti o certificati di singoli atti, il cui rilascio integra un trattamento per ragioni di giustizia, come tale non sottoposto alla generale regola riguardante il trattamento di dati da parte di soggetti pubblici (art. 27, l. n. 675/1996 cit.) né abrogato dalla stessa legge.

b) Con ricorso ex artt. 13 e 29, l. n. 675/1996, unitamente ad alcune doglianze nei confronti di una testata giornalistica, un interessato ha lamentato la pubblicazione su un quotidiano della notizia della richiesta del suo rinvio a giudizio (prospettando la violazione degli artt. 9 e 27 della legge, nonché dell'art. 329 c.p.p., da parte della competente procura della Repubblica e del magistrato inquirente), per il fatto che la notizia sarebbe stata fornita ai giornali prima della notifica al ricorrente della richiesta di rinvio a giudizio, e perciò opponendosi al trattamento dei suoi dati da parte della procura.

Per quanto relativo all'attività della procura e del magistrato, il ricorso è stato dichiarato inammissibile, perché né l'art. 13 (che disciplina i diritti dell'interessato e in particolare quello di opporsi al trattamento dei suoi dati), né l'art. 29 (relativo ai ricorsi), né l'art. 27 (sul trattamento di dati personali da parte di soggetti pubblici) rientrano tra le disposizioni che l'art. 4 della legge rende applicabili ai trattamenti per «ragioni di giustizia».

c) Il medico sociale di una società calcistica ha fatto presente che le cartelle cliniche di alcuni giocatori erano state acquisite dal procuratore della Repubblica che svolgeva un'indagine sul *doping* e ha presentato reclamo al Garante segnalando che:

- l'attività del magistrato non poteva ricomprendersi in quella disciplinata dal cit. art. 4 della l. n. 675/1996, non essendo possibile includere nelle ragioni di giustizia indagini di tipo conoscitivo volte alla ricerca di reati;
- nell'acquisire le cartelle il personale della ASL, aveva svolto funzioni di vigilanza amministrativa, anziché le funzioni di polizia giudiziaria che avrebbero consentito l'acquisizione;
- di non essere stato avvisato dello scopo in base al quale la documentazione medica veniva acquisita;
- le cartelle non erano state restituite, irrispettando, alla società sportiva che le aveva richieste.

Il Garante, disattendendo la qualificazione proposta dall'interessato, ha qualificato l'atto in base al suo significato complessivo, e cioè come reclamo anziché come ricorso. Ha rilevato poi che in base alle risultanze delle verbalizzazioni, il personale

della ASL aveva agito nell'esercizio di funzioni di polizia giudiziaria inerenti al procedimento penale seguito dal magistrato, sicché la sua attività rientrava nell'ambito di applicazione dell'art. 4, lett *e*) della l. n. 675/1996, relativa anche alla prevenzione di reati. Pertanto, rilevata la pertinenza dei dati all'indagine svolta, ed esclusa perciò la violazione degli artt. 4 e 9 cit., ha ritenuto di non dover dar seguito alla segnalazione.

d) In un altro caso, un interessato ha lamentato che alcuni dati relativi tra l'altro alla sua abitazione e a soggiorni alberghieri suoi e di familiari, figuravano agli atti di un'indagine penale alla quale egli era estraneo, e come tali erano stati poi pubblicati su organi di stampa.

Al riguardo il Garante, considerata in base all'art. 9 della legge l'applicabilità agli uffici giudiziari dei principi di pertinenza e non eccedenza dei dati trattati rispetto alle finalità perseguite, ha rilevato che alcuni degli elementi acclusi agli atti di indagine non avevano rilevanza procedimentale - ad esempio, i soggiorni di persone diverse presso il medesimo albergo in tempi assai distanti - ovvero venivano a essere riepilogati in forma equivoca, con riferimento a persone estranee all'inchiesta, tra cui minori e titolari di cariche istituzionali. Considerato altresì il pregiudizio derivante per i soggetti estranei dal deposito ai sensi del codice di procedura penale di tali atti di indagine, il Garante ha segnalato al Comando generale dell'Arma dei carabinieri alle cui dipendenze operavano gli organi che svolgevano l'indagine, nonché alle procure inquirenti, la necessità di conformare i trattamenti al disposto dell'art. 9 cit.

e) Particolare attenzione ha destato nell'opinione pubblica un'altra vicenda: sono state diffuse dalla polizia giudiziaria alcune informazioni (dati anagrafici, fotografia e ospedale di ricovero) relative a una prostituta, risultata sieropositiva. Nelle segnalazioni che hanno sottoposto la vicenda all'attenzione del Garante è stato tra l'altro richiamato l'art. 5, comma 4 della l. n. 135/1990 in materia di AIDS, in base al quale gli operatori sanitari possono comunicare i risultati di accertamenti diagnostici per infezione da HIV, di cui vengano a conoscenza nell'esercizio della professione, soltanto alla persona cui gli accertamenti sono riferiti.

Da informazioni acquisite presso la competente procura della Repubblica è emerso che questa, nell'ambito di indagini relative ai delitti di favoreggiamento, sfruttamento della prostituzione e tentate lesioni gravissime in danno di un numero indeterminato di persone, aveva autorizzato la polizia giudiziaria a rendere pubblici gli atti investigativi, affinché la diffusione del dato relativo allo stato di salute evitasse conseguenze ulteriori dei reati (art. 55 c.p.p.).

In proposito il Garante ha rilevato, in primo luogo, che le norme della l. n. 135/1990, pur non direttamente applicabili al caso di specie, devono essere considerate nel senso che l'ordinamento esige una particolare tutela per le informazioni inerenti ai casi di AIDS o di infezione HIV; ha quindi considerato non inerente alla propria competenza valutare se l'art. 55, c.p.p. fosse stato correttamente applicato e, in particolare, se fossero riconducibili a tale disposizione anche misure non tipizzate nel codice di procedura penale; ha poi esaminato la conformità del trattamento dei dati personali dell'interessata ai principi contenuti nell'art. 9 della l. n. 675/1996, .

Su questo punto, è stato segnalato alla questura e alla procura competenti che gli organi investigativi avrebbero dovuto individuare modalità e procedure di informazione più selettive e rispettose dei principi di pertinenza e non eccedenza dei dati (quali, per esempio, la divulgazione della notizia della sieropositività di una persona non contrassegnata con le relative generalità, indicando solo la zona in cui abitualmente si prostituiva, accompagnata da informazioni tramite numeri verdi o altri servizi «mirati»).

2.15 SERVIZI DI SICUREZZA E ATTIVITÀ DI POLIZIA

2.15.1 Trattamenti effettuati dal Ced del Dipartimento della pubblica sicurezza e dalle forze di polizia

La riforma della disciplina relativa ai trattamenti di dati effettuati dal Centro elaborazione dati del Dipartimento di pubblica sicurezza, operata con la l. n. 675/1996 (si veda l'art. 10 della l. n. 121/1981, come modificato dall'art. 42, comma 1, della l. n. 675/1996), ha portato a riconoscere agli interessati il diritto di accedere direttamente ai dati personali conservati presso lo stesso Ced, senza la necessità di motivare la richiesta e a prescindere dalla circostanza che l'erroneità, l'incompletezza o l'illecito trattamento dei dati emerga nel corso di un procedimento giurisdizionale o amministrativo.

Tale novità, consistente nell'eliminazione del necessario collegamento tra la pendenza di un procedimento e l'esercizio del diritto d'accesso (previsto invece nella vecchia formulazione dell'art. 10 della l. 1° aprile 1981, n. 121), ha determinato la necessità di fornire diversi chiarimenti, anche per l'anno 1998, nei confronti degli interessati che chiedevano l'intervento del Garante per accedere ai propri dati registrati nel Centro.

L'Autorità ha sollecitato in più occasioni i responsabili del Centro elaborazione dati a dare risposta, nei termini di legge, alle richieste pervenute (venti giorni: art. 42, comma 1, l. n. 675/1996). Nel corso di questa attività, il Garante ha constatato la collaborazione degli uffici dell'amministrazione del Ministero dell'interno, anche a livello periferico (spesso, infatti, la risposta agli interessati è stata fornita attraverso le questure), e una concordanza di opinioni sulla necessità di apportare alcune modifiche sostanziali alle procedure sino a ora adottate dal Dipartimento di Ps.

Tali modifiche appaiono necessarie per i trattamenti dei dati personali svolti sia dal Centro elaborazione dati, sia da tutte le forze di polizia (anche presso queste ultime il Garante ha svolto alcuni accertamenti, ai sensi degli artt. 31 e 32 della l. n. 675/1996), auspicandosi una loro introduzione attraverso i decreti delegati che dovranno essere emanati entro la fine di luglio 1999 (in attuazione dell'art. 1, comma 1, lettera i) della legge delega n. 676/1996, e della l. n. 344 del 6 ottobre 1998).

Nei provvedimenti adottati in questa materia, il Garante ha avuto modo di richiamare l'attenzione delle pubbliche autorità sulla portata dei principi sanciti dall'art. 9 della l. n. 675/1996 che trova applicazione, come è noto, anche nei confronti dei trattamenti svolti dai predetti soggetti (art. 4, comma 2, della stessa l. n. 675/1996) e, in particolare, sulla previsione relativa al periodo di conservazione dei dati contenuta al comma 1, lett. e) dello stesso articolo).

Va ricordato, a tale proposito, che la legge sulla *privacy* è la prima normativa italiana che riconosca e tuteli pienamente il diritto all'oblio, rimasto finora oggetto di frammentate pronunce della giurisprudenza e di un attento studio da parte della dottrina.

In base alle disposizioni contenute nell'art. 9 della legge, l'interessato ha quindi non solo il diritto di richiedere che i propri dati siano pertinenti e non eccedenti rispetto alle finalità perseguite, ma anche quello di poter esercitare, ove possibile, il proprio «diritto all'oblio», ossia il diritto che certi avvenimenti della propria vita, e situazioni personali non siano più oggetto di un trattamento di dati (nei limiti previsti dalla legge).

In linea con l'intento innovativo del legislatore del 1996, il Garante ha più volte evidenziato alle forze di polizia destinatarie dei propri interventi, l'importanza di tenere conto dei principi sopra esposti e, in particolare, di aggiornare i dati personali conservati nelle proprie banche dati, nonché di eliminare quei dati che risultino eccedenti rispetto alle finalità perseguite.

Il «diritto all'oblio» dell'interessato deve essere infatti tutelato specie quando avvenimenti quali il decorso del tempo (che a volte impone di non considerare più come reato l'illecito compiuto), o l'intervento di una sentenza di assoluzione dell'interessato, facciano mutare la posizione del singolo individuo, eliminando la necessità di detenere ulteriormente determinati dati.

2.15.2 Archivi N.SIS, Schengen e SIRENE

In base alla decisione dell'Autorità di controllo comune di Schengen del dicembre 1997, il Garante ha effettuato una verifica sulle misure di sicurezza adottate dal N.SIS e dall'ufficio SIRENE del Dipartimento della pubblica sicurezza, riferendone alla competente commissione parlamentare di controllo nel corso dell'audizione tenutasi il 12 marzo 1998.

Nel corso dell'anno, inoltre, il Garante ha ricevuto cinque richieste di verifiche da effettuare negli archivi N.SIS ai sensi dell'art. 11 della l. 30 settembre 1993, n. 388, di ratifica dell'Accordo e della Convenzione di Schengen, al fine di accertare l'eventuale presenza negli archivi di dati personali dei soggetti interessati - tutti cittadini non appartenenti a Paesi dello spazio Schengen - e la legittimità dei relativi trattamenti alla stregua dei principi contenuti nella richiamata Convenzione e nella l. n. 675/1996.

Delle richieste pervenute, tre sono state inoltrate per il tramite dell'Autorità nazionale di controllo francese (CNIL), una dall'Autorità ellenica e una direttamente dall'interessato.

2.15.3 Servizi di sicurezza

Le particolari caratteristiche e l'esito delle verifiche svolte all'inizio del 1998 hanno già avuto trattazione anticipata nella *Relazione per l'anno 1997*.

L'analisi delle peculiari implicazioni poste dal rapporto per la protezione dei dati e l'attività dei servizi di informazione e di sicurezza prosegue in maniera proficua e ha trovato un momento di sintesi nel mese di ottobre, in occasione della cerimonia di inaugurazione dell'anno accademico 1998-1999 della Scuola di Addestramento del SISDE e del discorso inaugurale che il Presidente dell'Autorità è stato invitato a svolgere su questi temi alla presenza del Ministro dell'interno e delle altre autorità presenti.

3 IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

3.1 COMPETENZE E ATTIVITÀ

3.1.1 Ricorsi

Come è noto, la l. n. 675/1996 ha apprestato una serie di meccanismi di tutela onde assicurare a tutti gli interessati la possibilità di far valere le situazioni soggettive da essa tutelate specificamente. Fra questi il procedimento più innovativo e rilevante è senza dubbio rappresentato al ricorso dal Garante previsto dall'art. 29 della legge.

Tale disposizione afferma che «i diritti di cui all'art. 1, comma 1, possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante. Il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria». Si tratta di un particolare genere di ricorso amministrativo che si pone in rapporto di alternatività con l'utilizzo dei comuni meccanismi di tipo giurisdizionale.

Nell'anno 1998 sono pervenuti al Garante un centinaio di ricorsi, che sono stati esaminati dall'Autorità. Al riguardo si deve rammentare che l'art. 33, comma 3, della legge affida all'apposito regolamento di organizzazione e funzionamento del Garante la previsione delle norme «concernenti il procedimento dinanzi al Garante di cui all'art. 29, commi da 1 a 5, secondo modalità tali da assicurare, nella speditezza del procedimento medesimo, il pieno rispetto del contraddittorio fra le parti interessate».

Poiché il citato regolamento è entrato in vigore solo il 16 febbraio 1999, il Garante ha dovuto individuare le modalità attraverso le quali rendere possibile, sul piano sostanziale, la tutela delle posizioni giuridiche cui è riferita la norma dell'art. 29. Al riguardo, l'Autorità ha operato tenendo presenti le coordinate di riferimento già individuate nelle prime decisioni assunte nel corso del 1997. Più specificamente, la prassi procedurale adottata ha seguito la linea già definita nel provvedimento del 16 ottobre 1997.

Poiché le regole del contraddittorio dovevano essere fissate nel citato regolamento, sarebbe risultato arbitrario che il Garante le avesse dettate autonomamente affrontando sul piano della mera prassi una delicata tematica attinente alle concrete modalità di esercizio dei diritti di difesa. Al tempo stesso, si doveva evitare un lungo stallo che avrebbe portato a non prendere in considerazione per diverso tempo istanze degli interessati che ipotizzavano violazioni di legge.

Alla luce di questa considerazione preliminare, nella fase transitoria che si è purtroppo prolungata per tutto il corso dell'anno, allo scopo di assicurare comunque la tutela di posizioni giuridiche soggettive delicate, si è valorizzato l'aspetto sostanziale degli atti presentati quali «ricorsi ex art. 29» e li si è qualificati e trattati come «reclami» ai sensi dell'art. 31 della legge. I reclami, infatti, possono essere esaminati anche senza contraddittorio e al di fuori dell'articolata procedura prevista dalla legge.

Ciò ha permesso di valorizzare la sostanza delle doglianze e di accertare i casi di trattamento non conformi alla l. n. 675/1996, senza sminuire le garanzie per gli interessati.

Peraltro, in sede di esame preliminare di tali istanze, si è comunque verificata la loro rispondenza ai previsti requisiti prescritti dall'art. 29. Nei casi di mancata rispondenza dei ricorsi ai cennati requisiti, il Garante ne ha dichiarato l'inammissibilità o, a seconda dei casi, la manifesta infondatezza, dal momento che l'accertamento di tali situazioni non richiede la necessaria instaurazione del contraddittorio.

L'esame delle decisioni adottate nell'anno 1998, porta a riscontrare, appunto, numerose declaratorie di inammissibilità. Nel primo periodo di applicazione della legge, infatti, sono pervenute numerose istanze, formulate ai sensi dell'art. 29, ma in realtà non corrispondenti ai parametri previsti dall'articolo medesimo. Spesso i ricorrenti non hanno, come richiede la norma, esercitato previamente i diritti di cui all'art. 13 della l. n. 675/1996, ma hanno adito immediatamente il Garante. In altre fattispecie non è stata data invece dimostrazione dell'eventualità che «il decorso del termine tra la richiesta al titolare o al responsabile del trattamento e la presentazione del ricorso (5 giorni previsti dall'art. 29, comma 1) avrebbe esposto taluno a pregiudizio imminente e irreparabile». Solo tale eventualità, se dimostrata, può giustificare l'immediata presentazione di un ricorso al Garante non preceduto dall'interpello del titolare o del responsabile.

Altre declaratorie di inammissibilità hanno riguardato invece l'impropria attivazione del meccanismo di tutela dell'art. 13 e del conseguente ricorso previsto dall'art. 29 in relazione ad ambiti che sono espressamente esclusi dall'applicazione dei suddetti articoli. Si ricordano, al riguardo, numerose richieste di accesso diretto presentate erroneamente nei confronti di soggetti pubblici operanti «per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati» o «per ragioni di giustizia, nell'ambito di uffici giudiziari, del Consiglio superiore della magistratura e del Ministero di grazia e giustizia» (art. 4, comma 1, l. n. 675/1996).

Altri casi hanno riguardato le ipotesi dell'art. 14 della legge, che non prevede, parimenti, l'accesso diretto dell'interessato nei confronti di trattamenti effettuati da determinati soggetti pubblici o in alcuni settori particolari (ad esempio: normativa antiriciclaggio, disciplina antiracket, trattamenti effettuati da commissioni parlamentari d'inchiesta, da soggetti operanti per finalità di tutela della politica monetaria e valutaria e del sistema dei pagamenti, nonché trattamenti riferiti all'indagine difensiva e all'esercizio di un diritto in sede giudiziaria).

Si è comunque precisato più volte che l'accertata inammissibilità del ricorso non pregiudica il diritto del ricorrente di rivolgersi al giudice ordinario per far accertare eventuali reati o per chiedere il risarcimento dei danni, anche morali, istanze in merito alle quali la l. n. 675/1996 non ha attribuito competenze al Garante.

Data la particolare novità dei meccanismi di tutela in questione era per molti aspetti fisiologico che la prima fase di applicazione della legge evidenziasse alcune incertezze o l'erronea utilizzazione degli strumenti di tutela.

Queste incertezze hanno però riguardato più gli aspetti formali (ad esempio, il mancato previo interpello del titolare) che quelli sostanziali di prospettazione di situazioni di illiceità o non correttezza. Ciò ha permesso al Garante di considerare comunque le violazioni prospettate anche nei casi di illiceità o di manifesta infondatezza, accertate le quali l'Autorità ha proceduto autonomamente, con separato provvedimento, a segnalare o a vietare determinate operazioni. Mentre appare ancora prematura una articolata analisi dell'utilizzo e dell'efficacia di questo nuovo strumento, l'esperienza del primo periodo applicativo segnala però alcuni temi preferenziali rispetto ai quali il contenzioso in materia di protezione dei dati personali si concentra.

Ad esempio, i casi più ricorrenti e significativi hanno riguardato il trattamento dei dati sensibili (specie in ambito sanitario) nonché l'uso dello strumento dell'art. 29 per contestare la correttezza di trattamenti svolti in ambito giornalistico. A questo proposito vanno segnalate alcune decisioni significative che, grazie alla tempestività dell'intervento, hanno contribuito a evitare l'ulteriore divulgazione di dati aventi particolare sensibilità.

In un primo caso si è vietato a una Commissione medica competente per gli accertamenti sanitari ex d.m. 8 maggio 1987, n. 187 (ad accertare, cioè, lo stato di inabilità a svolgere attività lavorative da parte di un pubblico dipendente), operante presso un ospedale militare, di comunicare a soggetti diversi dal ricorrente i dati relativi all'accertamento dell'AIDS e all'infezione da HIV. Nella circostanza, si è richiamato il puntuale disposto della l. 5 giugno 1990, n. 135 in materia di AIDS che impone un rigoroso obbligo di rispetto dell'anonimato quando siano in causa dati riguardanti, appunto, persone affette da AIDS. Tale legge è pienamente in vigore - come ricordato anche dall'art. 43, comma 2 della l. n. 675/1996 - e si pone in posizione di specialità rispetto ai più generali obblighi imposti, specie nella fase di transizione prevista dall'art. 41, comma 5 della legge, alle pubbliche amministrazioni nel trattamento dei dati sensibili (v. anche § 2.6.1). La questione esaminata è servita anche per richiamare l'attenzione dei Ministri competenti sulla necessità di adeguare il disposto del cit. d.m. del 1987 alle esigenze di tutela previste dalle ll. n. 135/1990 e n. 675/1996.

In un altro caso è stato invece ritenuto fondato il rilievo di una persona che lamentava la divulgazione su una rivista medica di radiografie a lei riferite, accompagnate dal suo nome di battesimo, dalla sua età e da indicazioni di carattere diagnostico. Il Garante ha affermato che tali elementi comportavano un trattamento di dati personali sensibili integrando il requisito dell'identificabilità del dato di cui all'art. 1, comma 2, lettera c) della legge. Ciò in ragione delle speciali circostanze legate al particolare nome di battesimo dell'interessato (nome straniero di non frequente utilizzazione), associato all'età della persona, nonché alla messa in circolazione di tali dati in un ambito territoriale ristretto (v. anche § 2.6.1).

Per quanto concerne l'ambito giornalistico, è risultata particolarmente significativa la decisione che ha portato all'accoglimento di un ricorso (qualificato, si è già detto, come reclamo) avente a oggetto la pubblicazione da parte di alcuni organi di stampa di articoli concernenti un fatto di cronaca e il connesso procedimento penale, che avevano visto protagonista un minore. La pubblicazione dei dati personali del minore coinvolto nell'incidente non è risultato essenziale ai fini dell'esercizio del diritto di cronaca. Più specificamente si è messo in luce come il chiaro dettato normativo dell'art. 13, comma 1 del d.P.R. n. 448/1988 vieti la pubblicazione e la divulgazione di notizie idonee a consentire l'identificazione del minorenne comunque coinvolto in un procedimento penale.

Si tratta di principi enunciati anche nella «Carta di Treviso» sottoscritta il 4/5 ottobre 1990 e che hanno trovato significativa conferma nel Codice deontologico dei giornalisti (pubblicato nella G.U. del 3 giugno 1998) entrato in vigore in data successiva alla presentazione del ricorso in questione.

Gli altri casi affrontati in sede di esame dei ricorsi sono illustrati nei paragrafi relativi alle singole tematiche.

La pubblicazione sulla «Gazzetta Ufficiale» (avvenuta il 1° febbraio 1999) del d.P.R. 31 marzo 1998, n. 501, recante il regolamento sull'organizzazione e il funzionamento dell'Ufficio del Garante, e la sua entrata in vigore il 16 febbraio successivo, ha apportato significative innovazioni alla procedura seguita per l'esame dei ricorsi.

Sono infatti entrate in vigore le norme, previste dall'art. 33, comma 3, della l. n. 675, che fissano con precisione le modalità di presentazione, il contenuto e il procedimento per tali ricorsi (artt. 18, 19 e 20, d.P.R. n. 501 cit.).

Inoltre, con deliberazione in data 18 febbraio 1999, il Garante ha fissato l'ammontare dei diritti di segreteria per la presentazione dei ricorsi (determinati in £ 50mila). L'ammontare contenuto di tali diritti vuole favorire l'accesso a questo particolare meccanismo di tutela, cui fa riscontro, altresì, la possibilità di prescindere da tale versamento qualora l'interessato si trovi nelle condizioni previste per l'ammissione al patrocinio a spese dello Stato, ai sensi dell'art. 3 della l. 30 luglio 1990, n. 217.

La normativa regolamentare ha demandato al Garante la determinazione dei casi in cui è possibile la regolarizzazione del ricorso. Questa Autorità ha provveduto in proposito con deliberazione in data 1° marzo 1999 (pubblicato in G.U. del 19 marzo 1999, n. 65) esplicitando una serie numerosa di ipotesi nelle quali la mancanza, nell'atto di ricorso, di alcuni elementi (incompletezza dei dati identificativi del ricorrente, del titolare o del responsabile o dell'eventuale procuratore speciale; indicazione dei motivi in maniera imprecisa o incompleta; assenza della prova del versamento dei diritti di segreteria, ecc.) può però portare alla successiva regolarizzazione dei ricorsi stessi. Il Garante si è inoltre riservata la possibilità di delineare ulteriori ipotesi di regolarizzazione anche alla luce dell'esperienza del primo periodo di applicazione delle nuove norme procedurali sui ricorsi.

3.1.2 Segnalazioni e reclami

Nell'anno 1998 sono pervenute al Garante numerose segnalazioni e reclami, presentati ai sensi dell'art. 31, comma 1, lett. d) della legge. Tali atti possono essere presentati senza bisogno di alcuna formalità e costituiscono una modalità molto agevole per permettere a tutti i cittadini di segnalare, appunto, violazioni della legge o comunque interessare il Garante rispetto a rilevanti problematiche che l'applicazione quotidiana delle norme pone in luce.

La trattazione di tali atti non è procedimentalizzata. Peraltro questa Autorità istruisce normalmente tali segnalazioni acquisendo in via preliminare ulteriori elementi di informazione e valutazione da parte dei titolari o dei responsabili del trattamento coinvolti nelle questioni di volta in volta esaminate. Il vaglio più completo della questione può portare poi anche all'adozione di provvedimenti di divieto, totale o parziale, del trattamento dei dati o di blocco degli stessi (art. 31, comma 1, lett. l), l. n. 675/1996).

In questi casi il Garante ha tratto lo spunto per fornire indicazioni concrete in ordine al trattamento dei dati nelle materie oggetto di segnalazione, dando spesso risalto di provvedimento di carattere generale ai casi che coinvolgevano un numero particolarmente ampio di interessati.

I procedimenti adottati dal Garante su tali segnalazioni sono illustrati nei vari capitoli della presente Relazione.

3.1.3 Attività consultive

3.1.3.1 *La consultazione da parte del Parlamento*

La legge non prevede specifiche consultazioni formali del Garante da parte del Parlamento. Ciononostante nel 1998 si sono registrate varie occasioni nelle quali al Garante è stato richiesto di formulare osservazioni e precisazioni, specie per inter-

pello da parte dei Presidenti delle commissioni parlamentari o in occasione di audizioni anche informali di rappresentanti dell'Autorità. Di queste occasioni si dà brevemente conto qui di seguito:

- *Comitato parlamentare di controllo sull'attuazione e il funzionamento della convenzione di applicazione dell'accordo di Schengen*: Audizione del Prof. S. Rodotà, presidente del Garante per la protezione dei dati personali, tenutasi il 12 marzo 1998.

- *Commissione parlamentare di vigilanza sull'anagrafe tributaria*: Indagine conoscitiva sui rapporti fra Ministero delle finanze e società concessionaria dei servizi informatici (SOGEI). Audizione del Prof. S. Rodotà, presidente del Garante per la protezione dei dati personali, tenutasi il 24 giugno 1998.

- *Commissione finanze della Camera*: Indagine conoscitiva sullo statuto dei diritti del contribuente (AC 4818). Audizione del Prof. S. Rodotà, presidente del Garante per la protezione dei dati personali, tenutasi l'8 luglio 1998.

- *Commissione giustizia del Senato*: Esame dello schema di decreto legislativo recante «Disciplina transitoria in materia di trattamento dei dati particolari da parte di soggetti pubblici». Audizione informale del Prof. U. De Siervo, componente del Garante per la protezione dei dati personali e del dr. G. Buttarelli, segretario generale, tenutasi il 4 novembre 1998.

- *Comitato ristretto istituito nell'ambito della Commissione affari esteri e comunitari della Camera*: Esame del disegno di legge di ratifica del Protocollo sulle immunità e i privilegi del personale di Europol (AC 4954). Audizione informale del Prof. S. Rodotà, presidente del Garante per la protezione dei dati personali, tenutasi il 27 gennaio 1999.

- *Commissione parlamentare di inchiesta sul fenomeno della mafia e delle altre associazioni criminali similari*: Audizione informale del Prof. S. Rodotà, presidente del Garante per la protezione dei dati personali, tenutasi il 24 febbraio 1999.

3.1.3.2 La consultazione da parte del Governo

In più occasioni, nel corso del 1998, il Garante ha poi esercitato la funzione consultiva prevista dall'art. 31, della l. n. 675/1996.

Il legislatore, prevedendo in particolare la consultazione del Garante da parte del Presidente del Consiglio dei ministri e di ciascun Ministro all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla legge (art. 31, comma 2), ha attribuito all'Autorità il compito di valutare preventivamente se nelle norme da emanare si ravvisino profili di contrasto o di disarmonia con i principi in materia di riservatezza.

La disciplina della consultazione obbligatoria, che attua il principio comunitario affermato nell'art. 28 della direttiva n. 95/46 CE, assume un'importanza fondamentale perché vi sia un'applicazione corretta e uniforme della legge nelle materie e nei settori che in numero sempre maggiore vengono peraltro disciplinati con fonti di normazione secondaria e con atti amministrativi.

Del resto, lo stesso legislatore ha mostrato di tenere ben conto della circostanza che la l. n. 675/1996 recava un complesso di principi innovativi che sarebbero andati a innestarsi su un preesistente ordinamento poco attento alle tematiche della riservatezza. E proprio per questo ha provveduto a predisporre appositi meccanismi per favorire un rapido adeguamento del sistema. Ne sono un esempio, sul piano normativo primario, l'affidamento al Governo della potestà legislativa delegata al fine di introdurre disposizioni integrative e correttive (l. 31 dicembre 1996, n. 676, artt. 1 e 2); a livello normativo secondario, la previsione di uno specifico ruolo attivo del Garante nei confronti del Governo (l. 31 dicembre 1996, n. 675, art. 31). La *ratio* che presiede all'attribuzione al Garante del compito di segnalare al Governo l'opportunità di

provvedimenti normativi richiesti dall'evoluzione del settore (l. n. 675/1996, art. 31, comma 1, lett. *m*)) è, poi, con ogni probabilità e a maggior ragione, la stessa che porta a disporre la consultazione del Garante da parte del Governo in ordine alla predisposizione di provvedimenti futuri (art. 31, comma 2).

Il parere dell'Autorità è stato richiesto, in particolare, sui seguenti provvedimenti:

- schema di regolamento per l'attuazione degli artt. 1, 2 e 3 della l. 15 maggio 1997, n. 127 (a cura della Presidenza del Consiglio dei ministri Dipartimento per gli affari giuridici e legislativi);

- schema di regolamento concernente le modalità di attuazione, accesso e adeguamento delle banche dati degli uffici del Dipartimento del territorio del Ministero delle finanze da parte dei comuni e degli esercenti la professione notarile (Ministero delle finanze);

- schema di regolamento recante la disciplina delle modalità di costruzione e tenuta del ruolo unico della dirigenza delle amministrazioni statali, anche a ordinamento autonomo, e della banca dati informatica della dirigenza, nonché delle modalità di elezione del componente del Comitato di Garanti (Presidenza del Consiglio dei ministri - Dipartimento per la funzione pubblica);

- schema di convenzione previsto dall'art. 17, comma 10, della l. 27 dicembre 1997, n. 449 per la riscossione delle tasse automobilistiche (Ministero delle finanze);

- schema di convenzione tra le Poste italiane Spa e il Ministero delle finanze per l'acquisizione dei dati relativi ai versamenti in conto corrente per le tasse sulle concessioni governative (Ministero delle finanze);

- schemi di convenzioni e di d.P.C.M. previsti dall'art. 17, commi 10, 11 e 12, della l. 27 dicembre 1997, n. 449 per la riscossione delle tasse automobilistiche (Ministero delle finanze);

- schema di decreto ministeriale recante il regolamento di individuazione delle malattie croniche e invalidanti ai sensi dell'art. 5 del d.lg. 29 aprile 1998, n. 124 (Ministero della sanità);

- schema di regolamento concernente il servizio di posta elettronica ibrida (Ministero delle comunicazioni);

- schema di regolamento per l'attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero (Ministero dell'interno);

- schema di regolamento per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato ai sensi dell'art. 133-bis della l. 15 maggio 1997, n. 127 (Presidenza del Consiglio dei ministri);

- schema di regolamento recante caratteristiche e modalità per il rilascio della carta d'identità elettronica e del documento di identità elettronico, a norma dell'art. 2, comma 10, della l. 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4 della l. 16 giugno 1998, n. 191 (Presidenza del Consiglio dei ministri).

- schema di decreto del Presidente della Repubblica recante regolamento istitutivo della carta dell'agricoltore e del pescatore e dell'anagrafe delle aziende agricole in attuazione dell'art. 14, comma 3, del decreto legislativo 30 aprile 1998, n. 173. (Ministero per le politiche agricole).

Il Garante ha constatato, per altro verso, di non essere stato consultato anche in quest'ultimo anno (per il 1997 cfr. la *Relazione per l'anno 1997*, pag. 57) su diversi atti normativi e amministrativi che pure interessavano da vicino la protezione dei dati personali e che contengono anche norme espresse in materia. In alcuni casi si è

giunti addirittura a dare per avvenuta una consultazione del Garante che però è mancata, o a prevedere il coinvolgimento o un ruolo per il Garante senza che l'Autorità fosse stata minimamente interpellata.

In più occasioni l'Autorità ha pertanto richiamato l'attenzione sul fatto che la mancata consultazione determina un vizio della procedura di adozione dei provvedimenti, che oltre a inficiare la validità dei provvedimenti adottati ha concretizzato, per la sua intensità, un fenomeno da segnalare doverosamente nella presente Relazione, nonché al Governo, ai Ministri interessati e alle autorità comunitarie. Queste osservazioni, unite all'auspicio che il Governo e i singoli ministeri osservino l'obbligo di consultazione in modo regolare e tempestivo, sono contenute già nella lettera del 27 gennaio 1998 indirizzata al Presidente del Consiglio dei ministri (cfr. Bollettino, n. 3, pag. 34).

Il rispetto dell'obbligo di preventiva consultazione è auspicato dal Garante non in termini di pura rivendicazione di competenze, ma su un piano di costruttiva cooperazione istituzionale, per accelerare il processo di adeguamento della normativa che influisce sulla protezione dei dati e per rendere meno gravosa la stessa attività delle amministrazioni interessate che potrebbero altrimenti trovarsi a dover successivamente modificare quanto eventualmente già disposto in contrasto con la normativa vigente in materia di *privacy*.

Il Garante non è stato consultato (in alcuni casi nonostante la menzione contenuta in epigrafe nel testo pubblicato in «Gazzetta Ufficiale»), nei seguenti casi:

- decreto del Direttore generale del Dipartimento delle entrate del Ministero delle finanze 18 marzo 1998, in materia di interscambio dei dati relativi all'ICI;
- decreto del Ministro dell'università e della ricerca scientifica e tecnologica 23 aprile 1998, relativo alle modalità di pre-iscrizione all'università;
- decreto del Ministro del lavoro e della previdenza sociale 8 maggio 1998, in materia di esercizio dell'attività di mediazione;
- decreto del Ministro dell'industria, del commercio e dell'artigianato 27 maggio 1998, in materia di certificati del registro delle imprese recanti la dicitura antimafia rilasciati dalle camere di commercio;
- decreto del Ministro dell'ambiente 4 agosto 1998, n. 372, recante il regolamento sulla riorganizzazione del catasto dei rifiuti;
- decreto del Ministero delle finanze 7 settembre 1998, n. 503, recante il regolamento in materia di fermo amministrativo di veicoli a motore e autoscafi, ai sensi dell'art. 91-bis del d.P.R. 29 settembre 1972, n. 602, introdotto con l'art. 5, comma 4, del d.l. 31 dicembre 1996, n. 669, convertito, con modificazioni, dalla l. 28 febbraio 1997, n. 30;
- d.P.R. 20 ottobre 1998, n. 428, regolamento recante norme per la gestione del protocollo informatico;
- d.P.R. 8 marzo 1999, n. 70, regolamento recante disciplina del telelavoro nelle pubbliche amministrazioni, a norma dell'art. 4, comma 3, della legge 16 giugno 1998, n. 191.

Il Garante, inoltre, è stato consultato tardivamente, ossia dopo la pubblicazione dell'atto sulla «Gazzetta Ufficiale», nei seguenti casi:

- regolamento in materia di contratti di locazione e di acquisto delle apparecchiature informatiche e sulle licenze d'uso dei programmi per elaboratore (in G.U. n. 302, 30 dicembre 1997);
- decreto del Direttore generale del Dipartimento delle entrate del Ministero delle finanze del 22 dicembre 1998 «Approvazione dei modelli di dichiarazione IVA concernenti l'anno 1998 con le relative istruzioni» (in Suppl. ord. alla G.U. 21 dicembre 1998, n. 297);

– decreto del Direttore generale del Dipartimento delle entrate del Ministero delle finanze del 22 dicembre 1998 «Integrazione dei dati da indicare, per il periodo d'imposta 1998, nella certificazione unica dei redditi di lavoro dipendente e assimilati» (in G.U. 30 dicembre 1998, n. 303).

Il Garante, confermando la piena disponibilità a fornire il proprio apporto al Governo e ai singoli ministri anche al di fuori dei casi di consultazione obbligatoria, ha formulato inoltre pareri su alcuni provvedimenti, e ha risposto a quesiti formulati dai diversi dicasteri. In particolare i seguenti atti:

– parere al Ministero dell'interno sulla disciplina relativa alla piena conoscibilità e pubblicità prevista per le liste elettorali (in Bollettino, n. 4, pag. 13);

– schema di decreto legislativo concernente la fissazione di criteri unificati di valutazione della situazione economica dei soggetti che richiedono prestazioni sociali agevolate nei confronti delle amministrazioni pubbliche Presidenza del Consiglio dei ministri, Dipartimento per gli affari giuridici e legislativi (in Bollettino, n. 4, pag. 35);

– schema di decreto legislativo concernente il riordino della partecipazione alla spesa sanitaria e delle relative esenzioni - Presidenza del Consiglio dei ministri, Dipartimento per gli affari giuridici e legislativi (in Bollettino, n. 4, pag. 39);

– risposta a un quesito formulato dal Dipartimento per la funzione pubblica in ordine alla possibilità di rendere pubblici gli elenchi nominativi dei dipendenti pubblici contenuti nell'anagrafe di cui all'art. 24, l. n. 412/1991 (in Bollettino, n. 4, pag. 44);

– atti collegati alla decisione su ricorso adottata rispetto alla tematica della busta contenente il modello «Unico 98», predisposto dal Ministero delle finanze per la presentazione della dichiarazione dei redditi (in Bollettino, n. 5, pag. 42);

– schema di convenzione con i concessionari del servizio di deposito, inventario e alienazione dei beni mobili iscritti in pubblici registri e sottoposti a confisca amministrativa Ministero delle finanze, su invito del Consiglio di Stato, nel parere n. 1298/87 del 21 ottobre 1997 Sez. III - (in Bollettino, n. 5, pag. 22);

– parere rilasciato al Ministero dell'interno relativo all'utilizzazione da parte di comuni e di corpi di polizia municipale di laboratori fotografici per lo sviluppo di fotografie da apparecchiature del tipo «autovelox»;

– nota al Ministero di grazia e giustizia in materia di notificazione degli atti giudiziari;

– risposta a un quesito formulato dal Ministero del lavoro e della previdenza sociale, in merito alla comunicazione e diffusione delle liste di mobilità;

– risposta a un quesito formulato dal Ministero del lavoro relativo alla «scheda di segnalazione sociale»;

– parere al Ministero di grazia e giustizia ai sensi dell'art. 15, comma 2, della l. n. 675/1996 sullo schema di regolamento recante norme in materia di misure di sicurezza minime;

– parere alla Presidenza del Consiglio dei ministri, Dipartimento per gli affari giuridici e legislativi, concernente la possibilità che l'Autorità garante della concorrenza e del mercato inserisca nei suoi provvedimenti definitivi la denominazione dell'associazione dei consumatori che ha segnalato gli atti di pubblicità ingannevole;

– parere al Ministero dell'interno concernente la richiesta di dati anagrafici da parte delle aziende sanitarie locali.

Nei pareri resi l'Autorità ha cercato di bilanciare le proprie funzioni di tutela e di garanzia con le esigenze di funzionalità perseguite dalle diverse normative di settore; in alcuni casi ciò ha comportato il suggerimento di modifiche al testo predi-

sposto, mentre in altri casi ha prodotto direttive e indicazioni da elaborare per giungere a una armonizzazione delle nuove norme con i principi in materia di riservatezza.

3.1.4 Autorizzazioni al trattamento dei dati sensibili

Le autorizzazioni, le decisioni sui ricorsi e i pareri sugli atti del Governo nelle materie incidenti sulla tutela delle persone e sulla riservatezza dei dati personali rappresentano gli atti attraverso i quali il Garante esercita le funzioni di maggior rilievo attribuitegli dalla l. n. 31 dicembre 1996, n. 675.

L'attività autorizzatoria, in particolare, ha per oggetto il trattamento dei dati sensibili da parte dei soggetti privati e degli enti pubblici economici (art. 22), il trattamento dei dati sulla salute da parte degli esercenti le professioni sanitarie e gli organismi sanitari pubblici (art. 23) e il trattamento di alcuni dati di carattere giudiziario (art. 24).

Sotto il profilo strutturale, il provvedimento autorizzatorio si compone di due elementi:

- il giudizio di conformità fra il trattamento dei dati oggetto di esame e le disposizioni contenute nella specifica normativa che disciplina l'attività o il comportamento del titolare (per esempio la legislazione lavoristica per il datore di lavoro), come pure nella normativa in materia di protezione di dati personali;
- la prescrizione, a carico del titolare del trattamento, relativa all'adozione di misure e accorgimenti a garanzia dell'interessato.

L'autorizzazione deve essere adottata, a istanza di parte o d'ufficio, in una fase temporale antecedente l'inizio del trattamento.

La presentazione della richiesta di autorizzazione segna l'inizio del procedimento, ossia il momento in cui nasce a carico dell'Autorità l'obbligo di provvedere nel termine di trenta giorni, trascorsi inutilmente i quali la mancata pronuncia equivale a rigetto.

3.1.4.1 Le autorizzazioni generali

Il Garante ha, altresì, la facoltà di esercitare d'ufficio la funzione autorizzatoria rispetto a categorie di titolari o di trattamenti attraverso le cd. autorizzazioni generali (art. 41, comma 7 come integrato dal d.lg. 9 maggio 1997, n. 123).

La formula autorizzatoria di carattere generale è stata utilizzata sin dal primo anno di applicazione della legge, in quanto ritenuta tecnica di amministrazione attiva più idonea rispetto al provvedimento individuale per contemperare gli interessi meritevoli di tutela di gruppi sociali ed economici omogenei e il diritto alla riservatezza.

Il Garante ha infatti adottato il 30 settembre u. s. sei nuove autorizzazioni generali al trattamento dei dati sensibili (v. Allegati, cap. 5.6):

- la n. 1/1998 relativa alla gestione dei rapporti di lavoro;
- la n. 2/1998 relativa ai dati sanitari e a quelli sulla vita sessuale;
- la n. 3/1998 relativa agli organismi di tipo associativo e alle fondazioni;
- la n. 4/1998 relativa ai liberi professionisti;
- la n. 5/1998 relativa a diverse categorie di titolari (settore bancario, creditizio, assicurativo, turistico, del trasporto, dei sondaggi e delle ricerche, della elaborazione dati, della selezione del personale e della mediazione a fini matrimoniali);
- la n. 6/1998 relativa agli investigatori privati.

Le nuove autorizzazioni, pubblicate sulla «Gazzetta Ufficiale» n. 229 del 1° ottobre 1998, non contengono mutamenti di carattere sostanziale rispetto alle precedenti, ma solo integrazioni o specificazioni sulla base dell'esperienza interpretativa e applicativa dei provvedimenti generali dell'anno precedente.

Anche in sede di rinnovo delle autorizzazioni generali, come in numerose altre occasioni, il Garante ha previamente sentito alcune parti interessate che ne hanno fatto richiesta e ha esaminato le istanze tempestivamente pervenute.

Alcune delle integrazioni apportate nelle nuove autorizzazioni sono infatti il risultato di valutazioni congiunte su questioni risultate poco chiare o profili non considerati nelle autorizzazioni dello scorso anno. A titolo meramente esemplificativo si riportano di seguito alcune delle citate modifiche.

In accoglimento di un'osservazione di Confindustria è stato ad esempio ampliato l'ambito di applicazione dell'autorizzazione relativa ai datori di lavoro ai trattamenti finalizzati all'adempimento di obblighi derivanti da contratti di assicurazione (cfr. il capo 3, lett. c) dell'autorizzazione n. 1/1998).

Su richiesta dell'Ordine degli psicologi, l'autorizzazione relativa al trattamento dei dati sulla salute è stata estesa agli psicologi in considerazione del fatto che la psicoanalisi presenta maggiori affinità con l'attività medica piuttosto che con quella, assai più eterogenea, dei liberi professionisti iscritti in albi o elenchi professionali (cfr. il capo 1, lett. a) dell'autorizzazione n. 2/1999).

È stato, inoltre, specificato che le imprese bancarie, creditizie o assicurative sono autorizzate al trattamento dei dati sensibili anche se in stato di liquidazione coatta amministrativa e ciò allo scopo di chiarire che l'attività svolta dal commissario liquidatore rientra nell'ambito di applicazione dell'autorizzazione (cfr. il capo I, punto 1), lett. a) dell'autorizzazione n. 5/1998).

Gli intenti perseguiti dal Garante attraverso lo strumento delle autorizzazioni generali sono stati, oltre quello già ricordato di uniformare a settori omogenei di attività le prescrizioni contenute nei provvedimenti autorizzatori, lo snellimento dell'azione amministrativa dell'ufficio del Garante e la semplificazione degli adempimenti a carico del titolare.

Tali preoccupazioni hanno indotto il Garante a disporre espressamente nelle sei autorizzazioni generali che i titolari dei trattamenti destinatari delle autorizzazioni generali non sono tenuti a presentare una specifica richiesta di autorizzazione se il trattamento effettuato è conforme alle prescrizioni ivi contenute, e a ricordare altresì che i soggetti pubblici possono continuare a trattare i dati sensibili sulla base di una disposizione transitoria e previa comunicazione al Garante (art. 41, comma 5).

I suindicati obiettivi sono stati, tuttavia, realizzati solo parzialmente. Nel 1998 sono infatti pervenute all'ufficio del Garante centinaia di richieste di autorizzazioni non dovute e relative sia a titolari o a trattamenti già considerati con le autorizzazioni generali, sia a enti pubblici. Tale situazione, per certi aspetti inaspettata perlomeno sotto il profilo della dimensione numerica, ha reso necessario un ulteriore impegno dell'Autorità nell'attività di divulgazione dei contenuti e delle corrette modalità di applicazione della normativa in materia di protezione dei dati personali.

L'Ufficio ha infatti provveduto a fornire specifiche informazioni a ciascuno dei richiedenti e ad allegare alle note di risposta la documentazione utile alla comprensione dei casi concreti.

Si aggiunge, inoltre, che le autorizzazioni generali conservano il carattere della provvisorietà temporale (hanno efficacia dal 1° ottobre 1998 al 30 settembre 1999), soprattutto in considerazione del fatto che la normativa in materia di protezione di dati personali dovrebbe essere integrata da alcuni decreti legislativi entro

il 31 luglio 1999, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa (cfr. art. 1 della l. 6 ottobre 1998, n. 344 sul differimento del termine per l'esercizio della delega prevista dalla l. n. 676/1996).

Per completezza è doveroso ricordare che nel periodo in cui furono adottate le autorizzazioni generali (settembre u.s.) la l. n. 344/1998 non era stata ancora approvata, essendo in corso d'esame in Parlamento il corrispondente disegno di legge governativo, poi divenuto legge il 6 ottobre u.s. Questa circostanza ha indotto il Garante a considerare la fase normativa attuale tuttora transitoria e a non adottare disposizioni autorizzatorie dettagliate, in modo da evitare che i titolari possano essere obbligati a modificare la propria attività in un breve periodo di tempo.

Per quanto attiene ai dati di carattere giudiziario si aggiunge, infine, che il Garante si è riservato di adottare un'autorizzazione generale sul trattamento di dati idonei a rivelare l'adozione di alcuni provvedimenti giudiziari a carico dell'interessato in previsione dell'emanazione di nuove disposizioni di legge in tale settore (art. 24, l. n. 675/1996; art. 686, commi 1, lett. a) e d), 2 e 3, c.p.p.).

Nelle more, una disposizione transitoria ha permesso ai soggetti pubblici e privati di proseguire il trattamento dei dati di cui all'art. 24 fino all'8 maggio 1999 previa comunicazione al Garante stesso (art. 41, comma 5 così come modificato dall'art. 1 del d.lg. n. 389/1998).

3.1.4.2 Le autorizzazioni ad hoc

Il Garante, nell'emanare le sei autorizzazioni generali citate, si è riservato di autorizzare trattamenti diversi da quelli già considerati soltanto in presenza di circostanze eccezionali. Nel 1998 ha accolto tre specifiche richieste di autorizzazione al trattamento dei dati sensibili.

Nel mese di gennaio l'Autorità ha autorizzato una società cooperativa di assicurazione a trattare i dati idonei a rivelare la convinzione religiosa dei soci limitatamente alle operazioni strettamente pertinenti all'applicazione di una disposizione statutaria della stessa società cooperativa che presuppone l'ammissione dei soli soci professanti la religione cattolica. Tale autorizzazione, rinnovata nel successivo mese di ottobre, è stata emanata alle medesime condizioni previste dall'autorizzazione generale relativa alle compagnie di assicurazione.

Il Garante ha poi autorizzato un istituto scolastico, in particolare una società a responsabilità limitata, a trattare i dati idonei a rilevare le convinzioni religiose degli studenti limitatamente ai dati e alle operazioni indispensabili all'applicazione della disposizione normativa che riconosce agli studenti di scegliere se avvalersi o no dell'insegnamento della religione cattolica (cfr. art. 310, d.lg. 16 aprile 1994, n. 297). Tale specifica disposizione autorizzatoria è stata in seguito recepita nel testo dell'autorizzazione generale n. 5/1998.

In sede di rinnovo delle autorizzazioni generali, l'ambito di applicazione del provvedimento relativo alle associazioni e fondazioni è stato esteso agli istituti scolastici, inclusi quelli di tipo non associativo, relativamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie all'applicazione della disposizione sulla libertà di scelta dell'insegnamento religioso (cfr. l'art. 310 cit. e il punto 1 dell'autorizzazione n. 3/1998).

Il Garante ha, infine, autorizzato una società per azioni a trattare i dati idonei a rivelare l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale dei propri clienti in modo strettamente funzionale all'adempimento degli obblighi contrattuali o precontrattuali derivanti da un rapporto di cui siano parte le predette associazioni od organizzazioni.

Anche in questo caso l'Autorità ha ritenuto meritevole di considerazione generale l'esigenza di garantire la gestione dei rapporti contrattuali tra gli operatori economici e le associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, e ha integrato in tal senso il testo dell'autorizzazione n. 3/1998 (cfr. il capo 1).

3.1.5 Rapporti con l'Ufficio del Garante

Seguendo uno stile adottato fin dal suo insediamento, l'Ufficio del Garante ha improntato, anche nell'anno 1998, la sua attività di relazione con il pubblico a criteri ispirati alla più ampia apertura e disponibilità. In questo quadro ha assunto un ruolo centrale il servizio di vero e proprio «sportello telefonico», che ha assorbito rilevanti risorse umane e temporali dell'Ufficio. È stata questa, peraltro, una modalità essenziale per cogliere dalla viva voce dei cittadini, degli operatori economici, dei funzionari delle pubbliche amministrazioni, il grado di conoscenza e attuazione della legge, i tempi, le modalità e le conseguenti difficoltà incontrate nel dare riscontro agli adempimenti normativi, nonché per raccogliere suggerimenti, segnalazioni e reclami.

In particolare, nei primi mesi dell'anno trascorso e soprattutto nel trimestre gennaio-marzo - in coincidenza con la scadenza dell'obbligo di notificazione del trattamento dei dati personali prevista dall'art. 41, comma 2 della l. n. 675/1996 - sono pervenute centinaia di chiamate telefoniche (si può stimare una media di 200 telefonate al giorno) e di richieste di informazioni inoltrate via fax, relative appunto alle modalità di adempimento degli obblighi citati.

Indubbiamente la novità e la particolarità della legge sulla protezione dei dati ha inciso su questa forte domanda di informazioni. Le chiamate erano volte ad avere conferma sui soggetti tenuti all'obbligo della notifica, anche in relazione ai numerosi casi di esonero previsti dall'art. 7, comma 5-ter della legge, a ottenere chiarimenti sulla apposita modulistica predisposta dal Garante, e sul rapporto fra il nuovo obbligo di notifica e la precedente denuncia di detenzione di archivi magnetici (introdotta dalla l. 1 aprile 1981, n. 121 e abrogata ora dall'art. 43, comma 1, della l. n. 675/1996).

In questa fase di consultazione intensa e quasi martellante dell'ufficio, le telefonate sono servite anche per mettere meglio a fuoco le problematiche e i dubbi più rilevanti e per orientare un'azione di più capillare informazione che ha fatto poi leva essenzialmente su comunicati stampa esplicativi, interventi a seminari e convegni organizzati particolarmente da associazioni professionali e di categoria, provvedimenti interpretativi assunti dall'organo collegiale e mirati a superare i dubbi più comuni. In questa fase si è cercato altresì di prendere contatto con coloro che avevano interessato l'Autorità a mezzo fax, fornendo, per quanto possibile, rapide indicazioni telefoniche e inviando, se necessario, documentazione di supporto.

Passato il periodo caratterizzato dalla «emergenza notificazioni», il flusso di richieste telefoniche è proseguito nei mesi successivi (con una media di 50 telefonate al giorno), nella fascia oraria dal lunedì al venerdì, dalle ore 10 alle 13, durante la quale i funzionari dell'ufficio (una decina al giorno) forniscono appunto consulenza telefonica. Come detto, tali telefonate sono un ottimo «termometro» sullo stato di «percezione» oltre che di attuazione della legge.

Da questa attività per certi aspetti ordinaria sono emerse alcune constatazioni e conferme che non appare banale riepilogare:

a) La materia della *privacy* intesa in senso lato interessa moltissimo la pubblica opinione, suscita emozioni e reazioni. Vi è però una diffusa difficoltà a cogliere la specificità della l. n. 675/1996 e a individuare con precisione i compiti e il ruolo del Garante. Anche il pubblico mediamente avvertito non coglie spesso lo specifico di una legge che mira alla protezione dei dati personali, mentre molte richieste di chiarimento prospettano generici problemi di salvaguardia della riservatezza della vita privata.

b) Per la natura stessa del suo oggetto (i dati personali) la l. n. 675/1996 ha un campo di applicazione e una forza di penetrazione assai ampi. Ciò spiega le difficoltà applicative incontrate dai soggetti, pubblici e privati, più diversi e giustifica, almeno in parte, la mole di richieste rivolte al Garante, visto come unico organo «specializzato» e titolato a fornire chiarimenti. L'esperienza ha messo, peraltro, in luce l'esistenza di «frontiere avanzate» dove il contatto fra i cittadini e la l. n. 675/1996 è particolarmente frequente e delicato. Non a caso centinaia di telefonate sono pervenute dagli enti locali, specialmente dai comuni, con particolare riguardo ai dati personali trattati negli archivi anagrafici e di stato civile, nell'archivio elettorale, nel settore dei servizi sociali globalmente intesi. Numerose sollecitazioni sono pervenute altresì dai soggetti, pubblici e privati, operanti nel campo sanitario (ASL in primo luogo) interessati, ovviamente, alle problematiche inerenti i dati sensibili.

c) Molte richieste sono state, invece, formulate da cittadini e da studi legali in ordine all'esatta configurazione dei meccanismi di tutela previsti dalla legge (ricorsi ex art. 29, segnalazioni e reclami ex art. 31). Le richieste telefoniche al riguardo miravano a conoscere, da una parte, la possibilità di valersi di tali strumenti, anche in assenza del regolamento di organizzazione e funzionamento del Garante di cui all'art. 33, comma 3 della legge, nonché tempi e modalità di trattazione dei medesimi procedimenti; dall'altra, a verificare la possibilità di ricondurre determinate fattispecie concrete ai citati strumenti di tutela.

L'esperienza di questi dodici mesi segnala indubbiamente l'utilità e la necessità di proseguire nell'impegno di disponibilità nei confronti delle molteplici richieste di informazione che quotidianamente pervengono, orientando i cittadini e gli operatori anche attraverso l'utilizzo di strumenti già disponibili (Bollettino, comunicati stampa, *newsletter*) o che sono in procinto di essere attivati (sito *Web*).

3.1.6 Registro generale dei trattamenti

3.1.6.1 Il quadro normativo

Per la tenuta del registro generale dei trattamenti la legge dispone l'impiego di sistemi automatizzati a elaborazione informatica e l'utilizzo di strumenti telematici (art. 31, comma 3), prevedendo inoltre opportune intese con le province e altre pubbliche amministrazioni per assicurarne la consultazione tramite strumenti informatici costituiti da almeno un terminale dislocato su base provinciale, preferibilmente nell'ufficio per le relazioni con il pubblico.

Per le notificazioni la legge ha previsto una procedura basata essenzialmente sull'invio a mezzo di lettera raccomandata o con altro mezzo idoneo a certificarne la ricezione, specificandone i contenuti essenziali (art. 7).

Il successivo d.lg. 28 luglio 1997, n. 255 ha modificato in parte l'art. 7 introducendo per alcune categorie un regime di notificazione semplificata - ad esempio per i soggetti pubblici e privati che effettuino trattamenti temporaneamente e senza l'ausilio di mezzi elettronici e automatizzati - esonerandoli dal menzionare alcuni dati

previsti per la generalità dei notificanti. Inoltre ha escluso numerosi soggetti dalla presentazione della notificazione, obbligandoli comunque a fornire le notizie sul trattamento dei dati a chiunque ne faccia richiesta.

Per quanto riguarda il termine per la presentazione della notifica per i trattamenti iniziati prima del 1° gennaio 1998, l'art. 2 ha individuato due date:

- 31 marzo 1998, per i
- trattamenti svolti anche in parte con l'ausilio dei mezzi elettronici o comunque automatizzati;
- trattamenti non automatizzati di dati sensibili o attinenti a determinati provvedimenti giudiziari;
- 30 giugno 1998, per i
- trattamenti non automatizzati di dati diversi da quelli sensibili;
- trattamenti effettuati per ragioni di giustizia, per il servizio del casellario giudiziale, per il servizio carichi pendenti, o da soggetti pubblici per finalità di difesa o sicurezza dello Stato o per finalità di prevenzione, accertamento o repressione dei reati.

Per tutti i trattamenti iniziati dal 1° gennaio 1998 è prevista la notificazione prima dell'inizio del trattamento. Ugualmente deve essere notificata al Garante la modifica degli elementi contenuti nella prima notificazione o la cessazione del trattamento dei dati. Sanzioni penali sono comminate in caso di omessa o infedele notificazione (art. 34, l. n. 675/1996).

Recentemente, poi, è entrato in vigore il d.P.R. 31 marzo 1998, n. 501 che agli artt. 12 e 13 ha introdotto norme integrative sulle procedure relative alle notificazioni, alla tenuta e consultazione del registro. In particolare, per quest'ultimo aspetto, l'art. 13 stabilisce che il registro è accessibile gratuitamente a chiunque senza particolari formalità presso l'Ufficio del Garante o mediante terminale.

3.1.6.2 L'organizzazione

Al fine di agevolare il compito di effettuare la notifica, il Garante ha predisposto modelli cartacei e supporti informatici, completi di varie spiegazioni, distribuiti gratuitamente in tutti gli uffici postali del territorio, in base ad apposita convenzione stipulata con l'Ente poste. A corredo sono state predisposte buste personalizzate complete di indirizzo, bollettini per il versamento dei diritti di segreteria (£ 15mila per notifica inviata su dischetto magnetico, £ 25mila per notifica inviata su modello cartaceo) e speciali buste imbottite per l'invio dei dischetti magnetici.

Complessivamente sono stati predisposti e consegnati tempestivamente agli Uffici postali per la distribuzione n. 1.020.000 modelli con allegate istruzioni e n. 350mila dischetti. Per agevolare ulteriormente la diffusione del modello, taluni organismi, associazioni ed editori sono stati autorizzati a riprodurlo sulla base di apposita convenzione stipulata con l'Ufficio, e il suo facsimile è stato pubblicato anche su alcuni giornali. In aggiunta, diversi comunicati stampa e le risposte fornite oralmente e via fax ai numerosi quesiti posti, hanno anch'essi agevolato il compito degli utenti nella compilazione del modello. Le notifiche pervenute sono state circa 250mila, in massima parte per posta o consegnate a mano e nella quasi totalità in occorrenza della prima scadenza del 31 marzo.

Le operazioni di preparazione delle notifiche per la successiva immissione dei dati nel sistema informativo si sono rivelate assai impegnative. Notevoli sono stati i problemi per fronteggiare una tale massa di documentazione, sia per le preliminari operazioni materiali da compiere (distacco e timbratura delle ricevute di ritorno, suddivisione tra modelli cartacei e dischi, apertura e verifica del contenuto dei plichi,

protocollazione, separazione delle notifiche *anomale*, inscatolamento e trasporto in una sede idonea a contenerle), sia per la mancanza di spazi adeguati al loro trattamento (il Garante si è successivamente avvalso di un locale di ampie dimensioni messo a disposizione gratuitamente dal Dipartimento della protezione civile presso il Centro polifunzionale in Castelnovo di Porto, che presenta tra l'altro adeguati livelli di sicurezza).

In tale luogo sono state effettuate in massima parte le operazioni propedeutiche alla verifica del contenuto dei plichi pervenuti e alle statistiche preliminari sul numero e la distribuzione tra dischetti e modelli cartacei, allo scopo di impostare un'adeguata organizzazione del lavoro.

Al fine di procedere celermente, in attesa della realizzazione del sistema informatizzato del Garante e di una dotazione organica di personale, è stato stipulato, a seguito di licitazione privata, un contratto con una società per la fornitura di due servizi complementari, diretto l'uno alla lavorazione preparatoria delle notifiche pervenute, l'altro alla loro memorizzazione. Adeguate misure sono state adottate per assicurare la sicurezza e la segretezza delle operazioni svolte.

Numerose sono state le notifiche - sia su dischetto sia su modello cartaceo - che per vari motivi non sono risultate complete o regolari (v. Tabella 2).

3.1.6.3 Prospettive

Nello scorso mese di febbraio si sono concluse le operazioni connesse alla verifica delle notifiche ed entro luglio sarà possibile attivare il registro dei trattamenti, con una prima fase sperimentale.

Verrà subito dopo verificata attentamente la possibilità dell'integrazione del registro dei trattamenti con la rete Internet per consentirne una consultazione agevole e funzionale, adottando le necessarie precauzioni affinché non sia pregiudicata la sicurezza e la riservatezza dei dati personali (ad esempio, mediante consultazioni di singoli nominativi di titolari di trattamento).

Con il completamento della disciplina sulla firma elettronica (in base al d.P.R. 10 novembre 1997, n. 513 e ai regolamenti previsti dall'art. 15, comma 2, della l. 15 marzo 1997, n. 59), sarà possibile poi varare un progetto che consentirà ai notificanti di effettuare o modificare la notificazione anche per via telematica (art. 12, comma 2, d.P.R. n. 501/1998).

L'esperienza acquisita servirà inoltre a elaborare un'interfaccia del dischetto contenente il software per la notificazione ancor più *user friendly*, per indurre i notificanti a privilegiare la modalità informatica rispetto al modello cartaceo.

Il registro dei trattamenti, una volta completato, sarà collegato a un servizio per la risoluzione di quesiti e permetterà di interloquire con il Garante anche al di là della mera acquisizione delle notizie sulla movimentazione del registro stesso, sulla distribuzione degli archivi, sull'ambito di comunicazione e diffusione dei dati, la natura dei dati oggetto del trattamento, le banche dati cui si riferisce il trattamento, i trasferimenti di dati all'estero, ecc.

I dati che seguono si riferiscono alle notifiche già memorizzate e, seppure riferiti a dati non ancora definitivi, offrono indicatori utili sul contenuto del registro e per l'organizzazione del lavoro.

Tabella 1 - Dati riepilogativi sulle notifiche

	Numero	%
Notificazioni pervenute al 19/1/99	250.000 circa	
di cui su modello cartaceo	195.000	88
di cui da dischetto	55.000	22
Notificazioni elaborate	117.000 circa	
di cui da modello cartaceo	65.000	55
di cui da dischetto	52.000	45

Delle notificazioni pervenute, 1.260 recano modifiche alla prima notificazione e 140 comunicano la cessazione del trattamento. Esse verranno memorizzate solo quando verrà completata l'elaborazione di tutte le prime notificazioni pervenute.

Inoltre, delle 250.000 notifiche pervenute può stimarsi che circa il 2% presentino irregolarità di vario genere. Per gran parte di esse è già stato rivolto ai notificanti l'invito a provvedere alla regolarizzazione.

La tabella seguente illustra i vari tipi di irregolarità riscontrate. La somma delle percentuali, al riguardo, è maggiore di 100 in quanto è possibile che in una notificazione siano presenti più irregolarità.

Tabella 2 - Tipologia delle irregolarità presenti nelle notificazioni pervenute

	%
Dischetto illeggibile (deteriorato, privo del <i>file</i> di dati, file diverso da quello richiesto)	43
Mancato versamento dei diritti di segreteria	31
Dischetti non accompagnati dalla relativa stampa	30
Mancata compilazione di tutti i riquadri del modello	16
Modello non conforme a quello prescritto	7
Mancata sottoscrizione del notificante	2
Altro	2

Va evidenziato infine che è in fase di valutazione anche la possibilità di permettere una consultazione più ampia del registro attraverso la diffusione di CD-ROM come avviene in Spagna. Il registro è pubblico ma i dati in esso contenuti, secondo quanto previsto espressamente dal d.P.R. n. 501/1998, potranno essere utilizzati solo per finalità di applicazione della normativa in materia di protezione dei dati (art 13 d.P.R. n. 501/1998).

Va precisato da ultimo che i modelli di notificazione già predisposti dal Garante nel 1997, una volta entrato in vigore il d.P.R. n. 501/1998, sono stati oggetto di un provvedimento del Garante che in data 18 febbraio 1999, una volta entrato in vigore il d.P.R. n. 501/1998, ha confermato i modelli stessi e l'ammontare dei relativi diritti di segreteria.

3.1.7 Attività ispettiva

La prima fase di applicazione della disciplina sulla protezione dei dati personali è stata caratterizzata dal maggior rilievo possibile dato all'informazione e alla comunicazione, nell'intento di favorire una piena conoscenza e visibilità di quei principi e valori che con la l. n. 675/1996 si è inteso tutelare, come pure al progressivo adeguamento alla legge stessa da parte dei soggetti chiamati ad applicarla. La linea seguita è stata quella della massima disponibilità e cooperazione nel fornire chiarimenti a dubbi di applicazione della normativa, nell'intento di far sì che la l. n. 675/1996 si ponesse più come un punto di partenza di un dibattito più ampio sulla protezione dei dati personali e il loro utilizzo, piuttosto che come una fredda elencazione di una serie di nuovi diritti, doveri e adempimenti.

Lo testimoniano la frequenza con cui negli ultimi mesi la l. n. 675/1996 e, ancor più spesso, un generico «diritto alla *privacy*» sono stati chiamati in causa. I quesiti posti telefonicamente e via fax ai funzionari, i comunicati stampa del Garante, gli articoli di stampa apparsi sull'argomento, e perfino le più fantasiose interpretazioni della l. n. 675/1996 o gli attacchi di cui è stata talvolta oggetto, sono serviti a dare contorni più definiti alla disciplina sulla protezione dei dati personali, all'esercizio dei diritti che ne derivano e, soprattutto, agli obblighi di legge e di correttezza.

I diritti contemplati e tutelati dalla l. n. 675/1996 - anche con previsioni di tipo sanzionatorio, amministrativo e penale - richiedono ora la creazione di una struttura dei controlli e la loro attivazione. Al di là delle scelte condivise di dare tempo alla l. n. 675/1996 per essere assimilata, compresa e completata, l'incompletezza derivata dalla mancanza di norme regolamentari ha fatto sì che, in assenza di una minuta disciplina riguardante le modalità di accesso e verifica, il settore dei controlli *in loco* non potesse decollare. Deve tenersi conto, poi, che il 1998 ha rappresentato un anno transitorio per l'ultimazione delle procedure previste per la notificazione del trattamento dati da parte dei soggetti interessati e per la creazione del registro generale dei trattamenti.

Il «Regolamento recante norme per l'organizzazione e il funzionamento dell'Ufficio del Garante», d.P.R. n. 501 del 31 marzo 1998, entrato in vigore solo il 16 febbraio 1999, all'art. 15 regola nel dettaglio le modalità di accesso e verifica, disciplinando così le modalità di svolgimento degli accertamenti previsti all'art. 32 della l. n. 675/1996. Il Garante, potendo disporre accessi alle banche dati, verifiche e ispezioni nei luoghi ove si svolge il trattamento dati, con la disciplina prevista all'art. 15 del Regolamento potrà rendere effettivi i controlli *in loco* e, in breve, possibili le prime rilevazioni. Le segnalazioni e gli esposti inviati al Garante in questi mesi, con-

siderate le caratteristiche delle notificazioni pervenute, forniscono un quadro già abbastanza definito di quali saranno i settori maggiormente interessati dagli accertamenti e dalle ispezioni da parte dell'Ufficio del Garante.

In primo luogo dobbiamo considerare che alcune significative banche dati, sia per il loro volume, sia, soprattutto, per il tipo di informazioni contenute, appartengono alla pubblica amministrazione nel suo complesso. Basti pensare ai dati trattati nel settore sanitario, della giustizia, in quello fiscale, dalle amministrazioni locali o raccolti dalle forze di polizia, solo per citarne alcuni. La pubblica amministrazione, in questo primo periodo di attività del Garante, considerando le attività svolte, la qualità dei dati raccolti e il numero di banche dati detenute, è stata oggetto di numerose segnalazioni in misura non inferiore a quella del settore privato.

Per quanto riguarda le imprese private, è stata l'attività bancaria, creditizia e assicurativa, con le attività connesse relative alla rilevazione dei rischi e al recupero dei crediti, ad attrarre il maggior numero di segnalazioni ed esposti. Seguono il settore della pubblicità diretta, i servizi telefonici, le attività di ricerca e selezione del personale, l'investigazione privata e la gestione di sondaggi e ricerche di mercato.

L'attività di accertamento e rilevazione dell'Ufficio del Garante si avvarrà - ma non necessariamente - delle segnalazioni e degli esposti di coloro che riterranno violati i loro diritti rispetto alla l. n. 675/1996. Una efficiente struttura dei controlli dovrà prevedere acquisizioni di notizie, ai sensi dell'art. 32 della legge - strumento largamente usato sin dalla prima fase della sua applicazione - e ispezioni settoriali, periodiche e d'ufficio, a banche dati pubbliche e private.

Le verifiche potranno comportare anche l'esame dei supporti informatici contenenti i dati personali, di sistemi di trasmissione e accesso ai dati, l'acquisizione di documentazione e informazioni pertinenti.

L'esercizio delle funzioni di controllo assegnate al Garante, gli accertamenti effettuati sulle banche dati, accanto alle violazioni amministrative e penali contemplate dalla l. n. 675/1996 (che se accertate daranno vita a procedimenti sanzionatori specifici), potranno anche, in positivo, comportare la segnalazione ai relativi titolari o responsabili delle modifiche più opportune per uniformare i trattamenti alle disposizioni vigenti. Nei casi più gravi, parallelamente all'avvio di procedimenti per violazione delle norme sulla protezione dei dati personali, si potrà avere anche l'applicazione di misure cautelari quali il blocco o il divieto, totali o parziali del trattamento dei dati.

Alla luce di tutto ciò risulta chiaro come l'attività di accertamento e ispezione sia un elemento fondamentale nel regime di garanzie previsto dalla l. n. 675/1996 a tutela dei diritti dei cittadini. La verifica sul posto della conformità dei trattamenti a quanto stabilito dalla legge, i poteri in ordine alla segnalazione delle modifiche da apportare, l'eventuale intervento sui trattamenti stessi, su impulso del Garante, trovano come preciso e giustificato contrappeso l'obbligo della segretezza, da parte del personale incaricato dall'ufficio del Garante, rispetto alle informazioni di cui esso potrà venire a conoscenza durante i rilievi e nell'esercizio delle proprie funzioni.

Al fine di rimuovere un ostacolo all'effettuazione degli accertamenti di cui all'art. 32 della l. n. 675/1996, nel corso dei quali possono emergere anche violazioni diverse da quelle amministrative, si è stabilito all'interno del decreto legislativo n. 51/1999 di conferire al personale addetto agli accertamenti, in numero non superiore a cinque unità, la qualifica di ufficiale o agente di polizia giudiziaria, limitatamente al servizio cui sono destinati e secondo le rispettive attribuzioni.

Tale previsione, e la necessità di una integrazione normativa, risultavano evidenti. Il fatto che, ad esempio, dagli accertamenti effettuati *in loco* con l'assenso del titolare o del responsabile o con l'autorizzazione del presidente del tribunale fossero rilevabili violazioni penali avrebbe imposto la necessità di interrompere gli accerta-

menti svolti fino a quel momento per richiedere la collaborazione di altri organi dello Stato, non per scelta operativa, ma come condizione necessaria per l'ultimazione e la legalità degli accertamenti in base al codice di procedura penale e alle relative norme di attuazione. Si è rimosso per questa via un non trascurabile impedimento, ferma restando la collaborazione e l'ausilio degli altri organi dello Stato in tutti quei casi in cui le situazioni ambientali e le caratteristiche specifiche degli accertamenti ne consiglino la richiesta e l'intervento.

3.2 L'UFFICIO DEL GARANTE

3.2.1 Regolamento sull'organizzazione e il funzionamento dell'Ufficio

Con il d.P.R. 31 marzo 1998, n. 501, è stato emanato il Regolamento recante norme per l'organizzazione e il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'art. 33, comma 3, della l. 31 dicembre 1996, n. 675.

L'originario testo del provvedimento, già emanato con d.P.R. del 31 marzo 1998, su conforme deliberazione del Consiglio dei ministri e su proposta del Presidente del Consiglio, dei Ministri di grazia e giustizia, tesoro, bilancio e programmazione economica e dell'interno, è stato oggetto di rilievi da parte della Corte dei Conti.

Con delibera collegiale della sezione del controllo del 23 luglio 1998, la Corte dei Conti aveva censurato otto disposizioni, concernenti sia la disciplina dell'organizzazione interna del Garante sia la materia, di carattere strettamente economico, concernente il trattamento del personale, del Presidente dell'Autorità e dei membri del Collegio.

L'organo di controllo accoglieva solo in parte le controdeduzioni formulate dalla Presidenza del Consiglio dei ministri con la collaborazione di questa Autorità, segnatamente quelle che chiarivano la portata di alcune disposizioni concernenti l'organizzazione interna del Garante e il funzionamento dell'Ufficio, e che prevedevano l'esercizio di alcuni poteri d'urgenza del Presidente (art. 5, commi 8 e 15, comma 3), mentre per le altre norme il Governo ha ritenuto di prestare acquiescenza alla deliberazione della sezione di controllo, con esclusione delle disposizioni di cui all'art. 6, comma 1, e all'art. 8.

Per tali due ultime disposizioni la Presidenza del Consiglio dei ministri ha richiesto alla Corte dei Conti (ai sensi dell'art. 25 del T.U.), il riesame del diniego di registrazione e, comunque, la registrazione con riserva, provvedimento adottato dall'organo di controllo con delibera delle sezioni riunite n. 1/E/99 del 22 gennaio 1999.

L'entrata in vigore del Regolamento determina una ulteriore amplificazione della tutela apprestata dall'ordinamento nei confronti dei trattamenti di dati personali effettuati in violazione della normativa sulla riservatezza, atteso che il provvedimento, come disposto dall'art. 33, comma 3 della l. n. 675/1996, contiene le disposizioni (individuabili nei capi V e VI) concernenti l'esercizio dei diritti dell'interessato (artt. 13 e 17 del regolamento, che attuano l'art. 13 della legge) e il procedimento per la presentazione e la decisione dei ricorsi all'Autorità (artt. 18-20 del regolamento, che attuano e integrano l'art. 29 della legge).

In virtù dell'istituzione del registro generale dei trattamenti, previsto dall'art. 31 della legge e disciplinato dall'art. 13 del regolamento, è reso effettivo il diritto di accedere gratuitamente, presso l'Ufficio o tramite terminali, a tutte le informazioni ottenibili dall'interessato in merito ai trattamenti notificati all'Autorità, mentre la puntuale disciplina dell'accesso esercitabile nei confronti del titolare del trattamento,

definita nell'art. 17, prevede una serie di agevolazioni che, pur semplificando l'esercizio del diritto stesso, tengono in debito conto l'esigenza del miglior temperamento con l'interesse alla speditezza della propria legittima attività da parte dello stesso soggetto titolare.

È ad esempio previsto che sia le richieste di accesso, sia le relative risposte, nonché la comunicazione dei dati rilevati, possano essere fornite oralmente, e che al titolare che non rilevi alcun dato personale relativo all'interessato nella propria banca dati, spetti un contributo spese per la ricerca effettuata, contenuto entro i costi della ricerca e non eccedente le 20mila lire.

Si è poi curato di svincolare il procedimento di richiesta di accesso da qualsiasi formalità, con la facoltà dell'interessato di avanzare la richiesta anche a una persona incaricata del trattamento, o facendosi assistere da una persona di sua fiducia e con la possibilità di trasmettere la richiesta anche via fax o per lettera raccomandata.

Per quanto concerne invece la disciplina dei ricorsi, il provvedimento rende operativa la tutela di cui all'art. 29 della legge, e l'effettività di una cognizione del ricorso alternativa a quella affidata al giudice ordinario e assistita da parallele garanzie. Queste sono: la facoltà di farsi assistere da un procuratore, la garanzia di un regolare contraddittorio e la possibilità di addivenire a una dichiarazione di non luogo a procedere in seguito a una spontanea adesione al ricorso da parte del titolare o del responsabile, a seguito del decorso del termine di tre giorni dalla comunicazione che l'Ufficio inoltra nei suoi confronti.

Di pari importanza, e del tutto strumentali alle disposizioni direttamente concernenti la tutela dei diritti riconosciuti dalla l. n. 675/1996, sono le disposizioni del Regolamento (artt. 15 e 16) attuative dei poteri di accertamento e controllo del Garante, nonché dei poteri inibitori che possono comportare l'emanazione di un provvedimento di blocco dei trattamenti.

Il Regolamento ha, in tale ambito, favorito chiaramente soluzioni che comportano una collaborazione dei soggetti interessati, e *in primis* del titolare e del responsabile, prevedendo la facoltà degli stessi di prestare il proprio assenso all'esercizio dei poteri di accesso che il Garante debba esercitare presso le loro banche dati (assenso che elimina la necessità di acquisire l'autorizzazione del presidente del Tribunale di cui all'art. 32, comma 3 della legge), e disponendo che il blocco del trattamento, previsto dalla legge in determinate ipotesi, possa essere effettuato tramite una procedura alternativa all'ordine autoritativo del Garante, e cioè direttamente dallo stesso titolare, su invito della Autorità, anche in contraddittorio con la persona interessata.

3.2.2 Il decreto legislativo concernente l'Ufficio

A decorrere dal mese di aprile del 1998 l'Autorità si è impegnata attivamente nel sottolineare l'esigenza di un rafforzamento dell'Ufficio e di una sistemazione stabile del trattamento giuridico ed economico del personale e ha offerto perciò il proprio contributo di studio e di riflessione al riguardo. Una parte della disposizione a ciò utilizzata era stata inserita nel decreto del 22 luglio più volte citato. Un secondo e più organico intervento normativo, che ha superato le disposizioni contenute nel decreto di luglio, ha avuto come scopo anche quello di richiamare l'attenzione sulla opportunità di un intervento di razionalizzazione più generale dell'assetto giuridico ed economico delle autorità indipendenti.

Lo schema di decreto, approvato in via preliminare dal Consiglio dei ministri il 3 dicembre 1998, una volta acquisito il parere delle competenti commissioni parlamentari (che hanno espresso parere favorevole formulando alcune osservazioni) è stato approvato in via definitiva dal Consiglio dei ministri il 19 febbraio 1999, con alcune modifiche che tengono conto dei suggerimenti formulati, appunto, dalle Commissioni affari costituzionali del Senato e della Camera.

In accoglimento di tali suggerimenti, il testo definitivo (d.lg. n. 51/1999, cit.) dà puntualmente conto di quali disposizioni siano «integrative» della l. 31 dicembre 1996, n. 675, (adottate, quindi, in attuazione dell'art. 1 della l. 31 dicembre 1996, n. 676, recante «Delega per l'emanazione di disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali») e quali siano invece «correttive» (emanate, cioè, in applicazione dell'art. 2 della medesima l. n. 676/1996).

In armonia con il predetto criterio sistematico, il suddetto schema consta di due parti. Nella prima, contenente le norme «integrative», si dà attuazione all'art. 1 della cit. legge delega n. 676/1996, la quale, alla lettera *c*), prevede la razionalizzazione del trattamento economico del personale del Garante per la protezione dei dati personali con quello del personale delle altre autorità amministrative indipendenti (secondo il tendenziale criterio dell'uniformità a parità di responsabilità costituzionale) e alla lettera *m*) del medesimo articolo prevede l'armonizzazione dello stato giuridico del personale del Garante con quello del personale dell'Autorità per l'informatica nella pubblica amministrazione (cui si applica, a sua volta, il trattamento economico dell'Autorità per le garanzie nelle comunicazioni: art. 42, comma 3, della l. n. 675/1996).

Nella seconda parte trovano invece collocazione le norme «correttive», in applicazione dell'art. 2, comma 1, lettera *b*) della stessa l. n. 676/1996, la quale conferisce al Governo la delega ad apportare le correzioni alla legislazione in materia di dati personali che si dimostrino necessarie per assicurarne la migliore attuazione.

Quanto al contenuto, lo schema di decreto legislativo affronta alcuni aspetti rilevanti.

Nell'art. 1 si istituisce il ruolo organico del personale dipendente del Garante e, in armonia con quanto previsto per altre autorità indipendenti, si demanda a un regolamento del Garante stesso la definizione dell'ordinamento delle carriere, delle modalità del reclutamento e dell'inquadramento del personale in servizio, nonché del trattamento giuridico ed economico.

Si prevede poi un trattamento economico provvisorio (corrispondente all'80% di quello attribuito al personale dell'Autorità per le garanzie nelle comunicazioni), il quale tiene conto del criterio della tendenziale uniformità del trattamento economico del personale dipendente dalle autorità indipendenti, come previsto dalla predetta lettera *c*) della citata legge delega, ma al tempo stesso della ragionevole esigenza, prima richiamata, di avviare una riflessione più generale sul tema stesso. Coerentemente con le predette esigenze, la soluzione cui si è giunti, sebbene comporti il riconoscimento al personale di un trattamento economico inferiore a quello previsto presso altre autorità indipendenti di pari rango istituzionale, tiene tuttavia conto non soltanto della posizione occupata nell'ordinamento dall'autorità, ma anche del criterio direttivo contenuto nella lettera *m*) della citata legge delega, secondo il quale lo stato giuridico del personale addetto all'ufficio del Garante deve armonizzarsi con quello del personale dipendente dell'Autorità per l'informatica nella pubblica amministrazione, cui si applica il trattamento economico in vigore per l'Autorità per le garanzie nelle comunicazioni. Per il periodo compreso tra l'8 maggio

1997 e la data di entrata in vigore del regolamento di cui sopra, lo schema di decreto prevede inoltre che resti ferma l'indennità di funzione corrisposta al personale, la cui entità è commisurata al 50% della retribuzione in godimento, con esclusione dell'indennità integrativa speciale, stabilendo altresì che, nelle more dell'inquadramento, l'indennità sia integrata poi dalla sola differenza tra la retribuzione in godimento (più l'indennità di funzione) e il futuro trattamento economico.

Si prevede, altresì, l'applicazione al Garante di alcuni istituti già presenti nell'ordinamento di altre autorità indipendenti, ma con una portata assai più limitata. In tale contesto si prevede, in particolare, la possibilità di assumere venti unità in posizione di fuori ruolo, che non possono superare il 20% delle qualifiche dirigenziali del nuovo ruolo e che comportano la contestuale mancata copertura di un corrispondente numero di posti in organico.

Nell'art. 2, nel rispetto della sfera di autonomia e di autorganizzazione tradizionalmente riconosciuta a tutte le autorità indipendenti, si attribuisce al Garante la potestà di ripartire fra le diverse qualifiche funzionali l'organico - fissato in cento unità - con proprio regolamento, in linea con i recenti sviluppi legislativi (v. in particolare le disposizioni del d.lg. n. 80/1998 sull'ARAN). Si attribuisce, inoltre, al Garante stesso il potere di autodisciplina interna anche per quanto concerne la riscossione e l'utilizzazione dei diritti di segreteria, nonché la gestione delle spese. A tal fine sono state apportate parziali modifiche all'art. 33, comma 3, della l. n. 675/1996, prevedendo il mantenimento del regolamento governativo per le materie che attengono, invece, al rapporto con il cittadino (es.: le norme concernenti il procedimento davanti al Garante, la disciplina del contraddittorio e le modalità della notificazione di cui all'art. 7 della legge).

Si prevede, inoltre, la possibilità di assumere un numero massimo di sole venti unità con contratto a tempo determinato (anziché, ad esempio, sessanta come previsto per l'Autorità per le garanzie nelle comunicazioni), precisando che tali unità comprendono gli eventuali consulenti assunti con contratto a tempo determinato.

Per altro aspetto, come si è già osservato nel par. 3.1.7, si riconosce a un numero limitato di addetti la qualifica di ufficiale o agente di polizia giudiziaria.

Si introducono, infine, due disposizioni già in vigore per altre autorità indipendenti, la prima tendente a chiarire i principi e le modalità di applicazione della l. n. 241 del 1990 e del d.lg. n. 29 del 1993, e la seconda volta a disciplinare la possibilità di utilizzare i consulenti anche con contratto a termine.

3.2.3 La gestione delle risorse umane

Il 1998 è stato un anno di transizione che si è caratterizzato per l'introduzione di alcune innovazioni che anticipano i futuri cambiamenti organizzativi.

Nelle more della definitiva approvazione del decreto legislativo che, tra l'altro, ha istituito il ruolo organico del personale dipendente del Garante (ampiamente illustrato in altra parte della relazione), il Garante si è avvalso del contingente, composto da dipendenti dello Stato o di altre amministrazioni pubbliche collocati fuori ruolo nelle forme previste dai rispettivi ordinamenti, messi a disposizione dalla l. n. 675/1996.

Attualmente prestano servizio presso l'Ufficio n. 39 unità, mentre per le restanti unità le relative procedure sono *in itinere*.

Sulla base dell'esperienza maturata nella fase di prima applicazione della legge, e su proposta del Garante, l'articolazione delle qualifiche originariamente prevista è stata leggermente modificata con il d.P.C.M. 29 aprile 1998 al fine di renderla maggiormente aderente alle esigenze funzionali dell'Autorità e alla mutata situazione relativa ai dipendenti nell'ordinamento di appartenenza.

Ciò ha consentito un apporto più consistente, rispetto alla originaria previsione, di funzionari da destinare alla delicata attività di promozione dell'applicazione della legge, nonché ai molteplici e crescenti compiti istituzionali. Le predette correzioni, lasciando invariato il contingente di personale a disposizione, non hanno tuttavia consentito di soddisfare appieno le esigenze organizzative che si sono andate manifestando nella prima fase di vita dell'Autorità. Al pieno raggiungimento di tale obiettivo, cui pure sono state dedicate notevoli energie lavorative, possono ora concorrere diverse condizioni, in modo particolare l'istituzione del ruolo organico del personale e il riconoscimento dell'autonomia organizzativa.

Il 1998 è stato un anno di transizione anche per altri e non secondari aspetti. La mancata pubblicazione del regolamento di cui all'art. 33 della l. n. 675/1996 non ha consentito di adottare, nelle more della razionalizzazione del trattamento economico e giuridico del personale, la disciplina transitoria dei rapporti di lavoro che hanno così continuato a rimanere soggetti alle norme contrattuali e legislative dei comparti di rispettiva appartenenza. Tanto meno è stato possibile affrontare le problematiche organizzative, formalizzando ruoli e funzioni.

Per altro aspetto, l'eterogeneità delle provenienze del personale non ha consentito l'utilizzazione e la conseguente corresponsione degli incentivi previsti dalla generalità dei contratti collettivi dei comparti pubblici, in assenza di criteri immediatamente applicabili al Garante. In relazione a ciò, il Garante ha proposto alla Presidenza del Consiglio dei ministri di chiedere un parere del Consiglio di Stato. Tale richiesta è stata pienamente condivisa dalla Presidenza stessa e attualmente si è in attesa che il Consiglio di Stato emetta il proprio parere.

Permanendo la situazione di incertezza sommariamente descritta, gli sforzi sono stati rivolti soprattutto alla definizione di programmi e obiettivi finalizzati al miglioramento dell'efficienza e dell'efficacia dell'azione svolta dall'Autorità. Nel contempo, soprattutto nell'ultimo scorcio del 1998, con alcuni provvedimenti sono state poste le premesse dei futuri sviluppi organizzativi.

In particolare, nelle more del parere del Consiglio di Stato cui si è accennato, è stato predisposto un provvedimento che definisce i caratteri dell'istituendo fondo di incentivazione, prevedendone l'articolazione in progetti obiettivi, peraltro già in atto in diversi ambiti dell'ufficio, e che pone i criteri di valutazione del grado di raggiungimento degli obiettivi e delle prestazioni individuali. Il provvedimento, tendenzialmente rivolto a organizzare l'attività lavorativa *per risultati*, istituisce inoltre un nucleo di valutazione, prefigurando il futuro servizio di controllo interno.

Con un altro provvedimento, si è prevista l'elaborazione di un piano di formazione finalizzato all'aggiornamento sulle tematiche attinenti alla protezione dei dati personali, nonché alla conoscenza e all'approfondimento delle lingue, in considerazione della dimensione europea e mondiale in cui si svolge l'attività del Garante. Si è così ritenuto, con un provvedimento di ampio respiro che stanziava a questo fine risorse finanziarie non indifferenti, di affermare in maniera non rituale il rilievo che il Garante riconosce alla formazione del personale.

Nel disegno organizzativo che si è andato delineando nel corso del 1998 e ancora allo stato embrionale, è apparso coerente disciplinare l'orario di lavoro sulla base di criteri di certezza della prestazione lavorativa e di flessibilità. Tali finalità

sono state raggiunte con l'attuazione del previsto sistema automatizzato di rilevazione delle presenze e la contestuale definizione del nuovo orario di lavoro (articolato su cinque giornate lavorative di sette ore e dodici minuti) che prevede una fascia oraria per l'ingresso abbastanza ampia. Con questa innovazione si è tentato di conciliare le esigenze organizzative con quelle personali e di coniugare il necessario rigore nell'accertamento dell'effettività della prestazione con i principi dell'autonomia e della responsabilità.

In sintesi, le scelte operate sono tese a prefigurare una organizzazione del lavoro attenta soprattutto agli obiettivi e alla qualità e, in coerenza con essa, la sostituzione dei controlli burocratici con più efficaci sistemi di valutazione dei risultati.

3.2.4 Codice etico

Il Garante per la protezione dei dati personali ha adottato un codice etico che, dal 1° luglio 1998, deve essere rispettato da tutti coloro che operano presso l'Ufficio.

Il codice specifica i doveri di lealtà, diligenza, operosità previsti per i dipendenti pubblici e dispone che l'attività svolta non solo sia ispirata ai principi di imparzialità, trasparenza e riservatezza, ma sia anche conforme alla particolare posizione di indipendenza riconosciuta al Garante e ai compiti di garanzia a esso affidati.

In tal modo il codice rappresenta un passo concreto e tempestivo per la definizione di canoni di etica professionale destinati a guidare l'attività quotidiana tanto nei suoi risvolti interni all'apparato, quanto nei riflessi esterni diretti al pubblico, secondo una generale linea di tendenza istituzionale che verosimilmente interesserà tutte le amministrazioni in un prossimo futuro.

Il codice etico tiene conto del fatto che il legislatore, anche attraverso l'istituzione del Garante, mira espressamente ad assicurare il rispetto della persona affinché il trattamento dei dati non giunga a ledere i diritti, le libertà fondamentali e la dignità delle persone. Pertanto il codice tiene conto del fatto che la chiara matrice «personalista» della legge e, insieme, la delicatezza della materia e la rapidità delle moderne tecnologie di trattamento dei dati conformano il modo di operare del Garante: prevede, quindi, non solo modalità di accesso e forme di intervento altrettanto dirette, rapide e sollecite, ma anche una condotta complessiva verso l'esterno particolarmente rispettosa delle situazioni personali dei soggetti coinvolti.

Per questo già alcune prime disposizioni generali del codice delineano una comunicazione con il pubblico improntata a cortesia, disponibilità, efficienza, in modo da determinare fiducia e collaborazione da parte dei soggetti che entrano in contatto con l'Ufficio.

Parallelamente, le medesime indicazioni, con formulazioni analoghe, valgono all'interno, con riferimento sia alle relazioni tra l'Ufficio e i dipendenti, sia ai rapporti tra colleghi.

Vengono indicati poi alcuni doveri specifici, collegati a principi e valori fondamentali.

Tra questi: l'imparzialità, che porta a evitare trattamenti di favore, pressioni indebite, situazioni di privilegio, condizionamenti, anche connessi all'adesione a partiti politici, sindacati, associazioni; l'integrità, per precludere il perseguimento di benefici personali e di profitti o interessi privati e mantenere piena autonomia di giudizio; la riservatezza, in ordine alle informazioni apprese e alle attività svolte, con particolare riguardo al segreto d'ufficio.

Attenzione specifica viene rivolta all'atteggiamento da tenere nei confronti degli organi di stampa e degli altri mezzi di informazione.

Infine hanno espressa trattazione le ipotesi di conflitto d'interessi con l'Ufficio, nelle loro varie manifestazioni.

In tal modo si sollecita un impegno a evitare comportamenti che comunque possano ingenerare sfiducia nel ruolo imparziale del Garante.

3.2.5 Attività seminariali

L'Autorità segue con particolare attenzione il dibattito scientifico, culturale e istituzionale sulle tematiche relative ai propri ambiti di applicazione. A tal fine sia i componenti del collegio, sia vari funzionari dell'Ufficio hanno partecipato a numerosi seminari e conferenze in Italia e all'estero su temi dedicati ai molteplici problemi connessi alla protezione dei dati personali. Tali occasioni hanno consentito di chiarire ruolo e natura della nuova istituzione, di analizzare e discutere il contesto culturale e istituzionale in cui essa opera e gli obiettivi che guidano i suoi interventi.

Anche l'attività seminariale si è svolta attraverso un'intensa partecipazione a convegni e incontri promossi da università, enti locali, aziende ospedaliere e istituti di credito, nonché da organismi associativi e organizzazioni di categoria cui è stato fornito di volta in volta il punto sull'attuazione della legge e sull'attività dell'Autorità, rendendo così meglio comprensibile il reale significato dei propri provvedimenti rispetto alle problematiche che da ciascun ambito sono state prospettate.

Il 3 aprile 1998, due giorni dopo la caduta delle ultime barriere al pieno inserimento dell'Italia nell'area di libera circolazione Schengen, il Garante ha partecipato al convegno promosso dal Comitato parlamentare di controllo sull'attuazione e il funzionamento della convenzione di Schengen sul tema «L'Italia e Schengen». In tale convegno il Segretario generale dell'Autorità ha svolto una relazione che affrontava la materia del rapporto fra Europol, SIS e uffici SIRENE e la protezione dei dati personali.

L'8 e il 9 maggio 1998 questa Autorità ha organizzato, poi, nella cornice di Palazzo Barberini a Roma, il convegno «Internet e *privacy* - quali regole?». L'iniziativa - che ha visto fra gli intervenuti importanti personalità fra le quali i commissari europei Monti e Bonino e il prof. Spiros Simitis - è servita a disegnare un quadro completo dei problemi della regolamentazione e dell'autoregolamentazione di Internet, facendo emergere che la tendenza alla globalizzazione rende vano tentare di orientare lo sviluppo della telematica basandosi sui soli contesti nazionali (gli atti del convegno sono pubblicati a cura della Presidenza del Consiglio dei ministri, Dipartimento per l'informazione e l'editoria, Roma, 1999). Sulla base di tali qualificati contributi si sta svolgendo un'ampia riflessione ai fini della predisposizione della disciplina normativa di settore.

3.2.6 Relazioni esterne, rapporti con i media

L'art. 31 della l. n. 675/1996 attribuisce al Garante, tra i suoi compiti specifici, quello di «promuovere la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità». È questo un compito di grande impegno, che evidenzia come le funzioni dell'Autorità si esplicino non solo attraverso azioni di vigilanza, controllo e, in generale, di regolazione, ma anche mediante interventi di promozione e diffusione del «valore *privacy*». Un compito legato, dunque, non solo alla necessità di adempiere alle funzioni istituzionali attribuite al Garante, ma anche all'obiettivo di perseguire una informazione corretta sui diversi ambiti della legge e sui nuovi diritti riconosciuti ai cittadini.

La comunicazione si pone, dunque, come un aspetto non secondario per un'Autorità che indirizza consapevolmente i suoi sforzi verso un'ampia e corretta informazione, finalizzata a rendere comprensibile il significato dei propri provvedimenti alle diverse articolazioni della società e a sviluppare, in tal modo, una cultura del rispetto. È in questo quadro che acquista particolare interesse e significato il rapporto diretto che l'Autorità intrattiene quotidianamente con i cittadini.

Proseguendo nella intensa attività di relazione con il pubblico avviata fino dagli immediati inizi della sua attività, il Garante ha assicurato un servizio di informazioni lungo tutto l'arco della giornata ai cittadini, agli organismi pubblici, alle imprese, che si presentano presso i propri uffici o effettuano richieste telefoniche per chiarimenti e indicazioni operative. Richieste e segnalazioni che risultano ancora numericamente elevate a riprova di un interesse sempre più diffuso nella società, così come di un'esigenza che, prima inespressa, ha trovato nell'istituzione dell'Autorità e nell'applicazione progressiva della legge sulla protezione dei dati gli strumenti per una sua affermazione. Le modalità informali e la facilità di contatto con i funzionari, promossa da parte dell'Autorità fin dalla sua entrata in funzione, hanno favorito non poco la possibilità di portare a conoscenza della società, in tutte le sue articolazioni, gli aspetti innovativi e cruciali della normativa sulla protezione dei dati e dei diritti che essa introduce nel nostro ordinamento e che riconosce a ogni cittadino.

Allo stesso modo viene assicurato un servizio di informazione e documentazione ai laureandi che intendano predisporre tesi di laurea sulle tematiche connesse alla tutela della *privacy*.

L'attività di comunicazione ai mezzi di informazione e l'utilizzo di diverse tipologie comunicazionali, così come delle risorse messe a disposizione da Internet, rappresentano l'altro veicolo di promozione, diffusione e chiarificazione della normativa sulla *privacy* e dei nuovi diritti riconosciuti alle persone, introdotti dalla l. n. 675/1996.

Teso verso una concezione del «comunicare per regolare», il lavoro svolto mediante i comunicati stampa e la divulgazione dei provvedimenti del Garante ha consentito di informare, in maniera semplice e puntuale al tempo stesso, sull'attività del Garante, sulle problematiche particolarmente delicate e rilevanti emerse nell'applicazione della legge, sugli aspetti nodali, di carattere giuridico, sociale, economico e culturale, affrontati dall'Autorità nell'interpretazione delle norme.

In quest'ambito vanno ricordate anche iniziative, innovative rispetto al panorama delle istituzioni pubbliche, che si sono concretizzate nella pubblicazione su quotidiani nazionali, prima del loro varo definitivo, di modelli di notificazione e di informativa per i quali sono stati richiesti ai cittadini, alle pubbliche amministrazioni, all'impresa privata, alle associazioni di categoria e agli organismi rappresentativi dei consumatori, suggerimenti e contributi finalizzati a una loro migliore definizione.

A distanza di due anni dall'entrata in vigore della l. n. 675/1996, l'impatto che il diritto alla riservatezza e al controllo dei propri dati ha avuto nel nostro Paese - coinvolgendo aspetti sostanziali della nostra società, dall'economia alla giustizia, alla pubblica amministrazione, ai comportamenti quotidiani, alla sfera culturale - ha assunto connotati di indubbia rilevanza.

Lo dimostrano le pur sintetiche statistiche elaborate dal Garante sulla presenza delle tematiche relative alla *privacy* sui mezzi di informazione. Basterà indicare qui alcune cifre: nel periodo che va dal marzo 1998 al marzo 1999, le pagine dedicate a questioni relative alla *privacy* dai maggiori giornali nazionali sono state oltre 2500, delle quali oltre 600 riguardanti specificatamente l'attività del Garante.

Da mettere in luce, tuttavia, nell'ultimo anno il persistere sulla stampa di vere e proprie «leggende metropolitane» derivanti dagli aspetti più di «colore» collegati al concetto di *privacy* e dallo spazio concesso a casi di eccessiva ed errata, quando non strumentale, interpretazione della legge. Queste «leggende» finiscono per ingenerare, nei cittadini come negli operatori, ingiustificati allarmi o pregiudizi infondati.

Una verifica, operata oltre che sul grado di attuazione della norma anche sul livello di comprensione e consapevolezza raggiunto da istituzioni, cittadini, pubblica amministrazione e sistema delle imprese, ha messo in luce l'esigenza di proseguire nell'impegno di chiarificazione e approfondimento sugli aspetti più complessi e delicati della legge sulla *privacy*.

In questa direzione, il Garante sta promuovendo iniziative e campagne di informazione ai cittadini attraverso diverse tipologie di media e forme di comunicazione mirata. Tra queste va ricordato il recente avvio di una *newsletter* settimanale che viene inviata alle redazioni degli organi di informazione, sia della carta stampata, sia dei media. La *newsletter*, redatta a cura del servizio stampa, si pone l'obiettivo di fornire in via continuativa e periodica un aggiornamento sull'attività dell'Autorità e di offrire uno strumento ulteriore di conoscenza e approfondimento delle tematiche connesse con la *privacy*.

Tra le attività di comunicazione va ricordata anche la pubblicazione a carattere bimestrale del bollettino «Cittadini e Società dell'Informazione» che, proseguendo nel cammino intrapreso all'indomani dell'entrata in vigore della legge, raccoglie i provvedimenti del Garante, la normativa in materia, i comunicati stampa e altra documentazione sull'attività dell'Autorità. Il bollettino, che viene inviato gratuitamente a chi ne fa richiesta, si è dimostrato uno strumento di approfondimento largamente richiesto sia da semplici cittadini che vogliono conoscere in maniera diretta l'attività del Garante, sia da quanti, funzionari pubblici, professionisti, imprenditori, intendano tenersi aggiornati sull'applicazione della normativa.

3.2.7 La gestione finanziaria

Con delibera del 29 aprile 1998, le risorse finanziarie a disposizione dell'Autorità sono state quantificate preventivamente in lire 15.045 milioni, di cui 12.045 milioni provenienti dal bilancio dello Stato (capitolo 4797 dello stato di previsione della spesa del Ministero del tesoro) e lire 3 miliardi provenienti dai diritti di segreteria versati dai soggetti che hanno notificato l'esistenza di un trattamento di dati personali, così come previsto dalla normativa.

Con successiva delibera del 10 dicembre 1998, il Collegio ha approvato una variazione al documento contabile di lire 2.700 milioni per maggiori accertamenti di entrata derivanti dai versamenti dei diritti di segreteria nel conto corrente postale aperto con le Poste Italiane Spa con la convenzione del 29 dicembre 1997. A tale aumento di entrate ha fatto riscontro un corrispondente incremento di spese con la creazione di un apposito capitolo il cui stanziamento è utilizzato per affrontare gli oneri derivanti dalla istituzione e tenuta del registro generale dei trattamenti sulla base delle notificazioni ricevute, così come prescritto dall'art. 31, comma 1, della l. n. 675/1996.

Per l'esercizio 1998 le risorse a disposizione del Garante sono così ammontate complessivamente a lire 17.745 milioni.

Il documento di programmazione finanziaria per il 1998, redatto ai sensi dell'art. 3 del d.P.C.M. 6 ottobre 1994, n. 769, ha previsto alcuni settori strategici d'intervento sui quali far affluire le risorse a disposizione. Sede del Garante, sistema in-

formatico, biblioteca, attività connessa a seminari, convegni e incontri, acquisto di beni e servizi, spese per il personale e gli organi istituzionali sono stati i settori prioritari sui quali si è approntato il documento contabile.

Alle spese di funzionamento dell'ufficio del Garante si è provveduto già dall'esercizio 1997 con l'apertura di una contabilità speciale presso la Banca d'Italia Tesoreria Provinciale dello Stato Sezione di Roma, sulla quale sono confluiti, in entrata, i fondi derivanti dal Tesoro e quelli provenienti dal trasferimento dal conto corrente postale. Alle spese si provvede con la emissione di ordinativi tratti sulla stessa contabilità speciale, intestati ai legittimi creditori.

A seguito di questa impostazione la gestione finanziaria ha avuto un percorso senza eccessivi problemi, anche se la fase di assestamento organizzativo delle risorse umane e materiali dell'Autorità non è stata ancora raggiunta.

Durante l'esercizio 1998 i pagamenti sono risultati inferiori a lire 5.500 milioni di cui oltre 400 milioni di lire per spese relative a impegni dell'esercizio 1997.

L'indennità spettante al Presidente ai sensi dell'art. 30, comma 6 della l. n. 675/1996, è stata liquidata per un ammontare lordo di lire 357.892.472. Agli altri tre componenti il Collegio, come disposto dalla stessa norma, l'indennità liquidata è stata pari ai due terzi (238.594.980 lire lorde) di quella spettante al Presidente. L'onere complessivo per l'indennità ai componenti il Collegio del Garante è risultato di lire 1.073.677.412 per l'esercizio 1998.

I compensi accessori al personale distaccato presso il Garante in base all'art. 33, comma 1 della l. n. 675/1996, sono stati liquidati per un ammontare di lire 859.084.496 lorde a cui debbono aggiungersi gli oneri residui per la restituzione dei trattamenti che, alla approvazione definitiva del ruolo dell'Ufficio del Garante, saranno richiesti dalle amministrazioni di appartenenza. I 22 milioni di lire pro-capite non sono quindi una cifra rilevante sotto il profilo finanziario, se si tiene conto delle qualifiche del personale distaccato (sei dirigenti, tre IX livelli, dieci VIII livelli). L'unico dato che va chiarito concerne il consistente ricorso all'istituto del lavoro straordinario (500 milioni), che si è reso assolutamente necessario al fine di poter fronteggiare l'enorme carico di lavoro con le poche risorse umane a disposizione.

Nel corso del 1998 il Garante ha organizzato il convegno «Internet e *privacy*: quali regole» che si è svolto a Roma l'8 e il 9 maggio, con la partecipazione di rappresentanti esteri di istituzioni similari e di eminenti studiosi della materia. Il costo del convegno ha superato di poco lire 240 milioni. Con tale cifra sono state coperte tutte le spese: affidamento dell'incarico di organizzare il convegno a una società del settore, compenso per la collaborazione ai relatori esteri e nazionali, viaggio e soggiorno degli stessi, stampa degli atti da distribuire durante il convegno, spese telefoniche e telematiche (teleconferenza).

All'inizio del 1998, l'Autorità ha preso possesso di una nuova sede, affittata da privati, ristrutturata e arredata con il fattivo e professionale intervento del Provveditorato generale dello Stato. La dimensione della sede (circa 500 mq), però, non era tale da poter rappresentare l'unica e definitiva sistemazione del Garante. Si è così provveduto, come si dirà, dopo attente ricerche di mercato, a individuare locali più ampi e più rispondenti alle necessità dell'Autorità. Le spese per i canoni di locazione della sede attuale hanno comportato un esborso di lire 158.818.500, mentre per i lavori di ristrutturazione la spesa congruita è stata di quasi 300 milioni di lire. Le risorse non spese nell'anno 1998 sullo stanziamento previsto (4,2 miliardi di lire) consentono al Garante di poter impegnare cifre ragguardevoli per gli oneri di locazione e l'adattamento dei locali della nuova e definitiva sede dell'Autorità.

Particolare cura ha riservato il Garante all'acquisto di libri e riviste sui temi propri della *privacy*. Le risorse stanziare per la nascente biblioteca, che sarà parte importante del «Centro di documentazione multimediale» e che troverà sistemazione nei locali disponibili nella futura sede, hanno consentito già l'acquisto di pubblicazioni italiane ed estere per oltre 150 milioni di lire di cui circa 80 milioni spese durante l'anno.

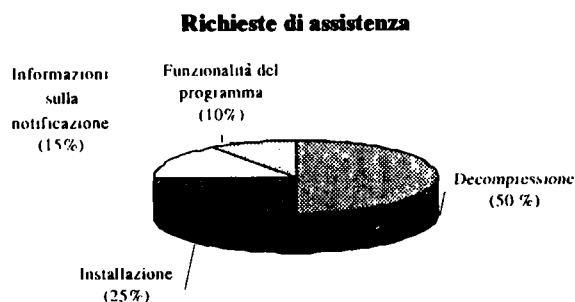
A fine anno, le risorse ancora disponibili sono state oggetto d'impegno mediante delibere finalizzate interessanti il settore informatico, compresa l'apertura del sito *Web*, il settore del registro dei trattamenti e il recepimento degli istituti del Contratto collettivo nazionale di lavoro del personale delle amministrazioni cui appartengono i dipendenti attualmente in servizio presso il Garante.

La gestione amministrativo-contabile delle risorse si è mossa lungo le direttrici tracciate dal documento programmatico finanziario assecondando il raggiungimento degli obiettivi istituzionali perseguiti dal Garante.

3.2.8 Informatizzazione

Le tecnologie dell'informazione, seppure in un quadro di ridotta disponibilità di risorse umane, hanno avuto nel corso del 1998 un ruolo significativo soprattutto nei rapporti tra l'Ufficio del Garante e l'utenza.

Va ricordato infatti che la predisposizione di un programma informatico per le notificazioni di trattamenti di dati personali in formato elettronico, al di là del lavoro svolto per l'analisi e la realizzazione del programma stesso, ha comportato la necessità di svolgere un servizio significativo in termini di assistenza agli utenti, servizio per certi aspetti di portata inattesa e determinata dalla diffusione del programma via Internet effettuata da soggetti convenzionati con il Garante. Tale forma di diffusione del programma si è affiancata a quella principale prevista dal Garante che è consistita nella distribuzione dei modelli cartacei e dei floppy disk contenenti il programma stesso attraverso gli uffici postali, possibile grazie alla stipula di un'apposita convenzione con l'Ente Poste Spa¹⁾.



1) Il servizio di assistenza ha presentato caratteristiche dimensionali e di contenuti del tutto inattese al momento della programmazione del lavoro. Il 50% delle richieste di assistenza ha riguardato le procedure di decompressione del programma posto su siti *Web* e il 25% le procedure di installazione del programma sul personal computer.

Considerando una media di circa cento richieste telefoniche al giorno per il periodo gennaio-ottobre, si può affermare che siano pervenute complessivamente non meno di 20mila richieste di assistenza per il solo servizio delle notificazioni. Tale carico di lavoro ha rappresentato una quota non trascurabile della più generale attività volta alla predisposizione del registro generale dei trattamenti.

Parallelamente si è provveduto alla progettazione architeturale e dimensionale dell'elaboratore server necessario a ospitare il registro in formato elettronico. Tale attività, condotta con l'ausilio di una apposita Commissione di esperti, ha consentito l'espletamento di una gara per l'acquisizione del server e dei servizi connessi.

Attività per l'organizzazione interna

Il regolamento che disciplina l'organizzazione e il funzionamento dell'Ufficio del Garante prevede «che l'Ufficio operi, di regola, mediante strumenti informatici e telematici» (art. 7, comma 2, lett. e), del d.P.R. 31 marzo 1998, n. 501). Pertanto, e anche allo scopo di favorire lo sviluppo dell'Ufficio del Garante in piena armonia con l'innovazione tecnologica, nei primi mesi del 1998 si è provveduto a completare le dotazioni di strumenti informatici a tutto il personale in servizio. Ogni operatore dispone pertanto di personal computer dell'ultima generazione, completo di accessori e dotato di strumenti software per l'informatica individuale praticamente completi rispetto allo stato dell'arte.

Tali dotazioni consentono la predisposizione dei documenti interni del Garante in formato elettronico, favorendo altresì lo sviluppo del sistema informativo automatizzato basato su una organizzazione efficace.

È previsto infatti che tali strumenti tecnologici siano collegati tra loro in rete locale e collochino con un elaboratore server detto «di stage» idoneo a predisporre in modo semiautomatico la documentazione di alimentazione del sito *Web* del Garante per il quale è in corso la procedura di realizzazione.

Tra le prime applicazioni gestite in rete locale va menzionata la gestione automatica del protocollo d'archivio. Nel corso del 1998 sono stati protocollati circa 10mila documenti e grazie all'uso della tecnologia è stato possibile estrarre alcuni rapporti di natura statistica, volti a determinare principalmente lo stato di trattazione delle pratiche, i carichi di lavoro e la distribuzione per tipologia di documento. Un nuovo sistema di protocollo è attualmente in fase di sperimentazione, in linea con le indicazioni del recente d.P.R. 20 ottobre 1998, n. 428, per la gestione del protocollo informatico da parte delle amministrazioni pubbliche.

Sito Web e servizi di connettività in rete

Il 1998 è stato un anno significativo per l'impostazione tecnologica dell'architettura del Garante. A più riprese e con significativi contributi di tecnici esperti, appositamente nominati, si sono analizzati i fabbisogni di tecnologie, anche in relazione alle funzionalità ritenute necessarie, e sono state definite le linee guida per lo sviluppo del sistema.

Ciò, anche in relazione a quanto già consolidato in organismi omologhi a livello internazionale, ha condotto alla scelta di tecnologie Internet (in particolare la *suite*

dei protocolli TCP/IP, peraltro come è noto in evoluzione) per sviluppare il sistema informativo. Le suddette tecnologie rappresentano oramai un consolidato standard di mercato, e risultano certamente economiche e facilmente disponibili anche in termini di disponibilità delle relative risorse professionali.

Dopo i necessari approfondimenti sono state condotte due indagini di mercato che hanno consentito la definizione delle caratteristiche del sito *Web* del Garante che potrà essere realizzato e messo in linea nel entro il giugno del 1999.

Parallelamente, anche per la gestione dello stesso sito *Web* in linea, sono stati definiti in termini di prestazioni e tecnologie di sicurezza i servizi di connettività necessari al Garante per completare la propria organizzazione tecnologica. Non va infatti dimenticato che se è di fondamentale importanza fornire all'utenza un servizio informativo completo ed efficace di natura elettronica, è oltremodo importante che il personale del Garante possa accedere alla rete Internet per soddisfare i propri fabbisogni informativi, soprattutto a livello internazionale. Non si deve poi trascurare l'efficacia dei servizi di posta elettronica e di trasferimento di *file* per favorire tempestività ed efficienza nell'attività quotidiana.

Da ultimo, va sottolineata la stretta correlazione esistente tra le attività tecnologiche in corso di sviluppo e i benefici che tali attività potranno portare alla costituzione e alla gestione dell'Ufficio per le relazioni con il pubblico, prevista per la fine del 1999, e alla costituzione e gestione di un servizio di documentazione e di biblioteca. A tale ultimo servizio il Garante ha attribuito notevole importanza ai fini dello sviluppo della cultura della *privacy* nel nostro Paese.

3.2.9 Creazione di un Centro di documentazione

La vasta quantità di materiale documentale concernente la protezione dei dati rende opportuna la costituzione di un Centro di raccolta, di selezione e di catalogazione con funzione di archivio a supporto delle attività del Garante.

Il nucleo di base di questo Centro di documentazione consisterà delle seguenti dotazioni:

- biblioteca, con libri e riviste giuridiche d'interesse;
- stazioni anche multimediali di lavoro;
- notiziario con lo spoglio di articoli di riviste italiane specializzate, la segnalazione di convegni e seminari e il riversamento di documenti dai siti Internet;
- rassegne stampa italiana ed estera;
- osservatori su temi specifici condotti su periodici nazionali e internazionali specializzati.

Le collezioni delle rassegne, degli osservatori e dei notiziari coincidono solo in parte con una tipologia di documentazione destinata esclusivamente a uso interno. Anche sul piano del materiale documentale ricavato dalla stampa quotidiana, l'archiviazione si estende infatti a campi, temi e situazioni che oltrepassano il raggio di iniziative messe già in opera dal Garante, disegnando orizzonti e scenari possibili per la ideazione di nuovi interventi (in questo senso è stata indicativa la raccolta di materiali per l'iniziativa sulla video-sorveglianza, v. § 2.12.2).

A questo riguardo, si è avviata una schedatura della totalità del materiale documentale con un sistema di catalogazione messo a punto con l'apporto dell'Istituto per la Documentazione Giuridica (Cnr) e degli Archivi di Stato per la classificazione degli atti amministrativi dell'Ufficio. L'adozione di questo criterio scientifico di indicizzazione e di archiviazione consente di trasferire in una banca dati «aperta» (perché quotidianamente incrementabile) la documentazione, anche giuridica, le notizie e gli articoli di stampa selezionati a fini di informazione. In tal modo la funzione classificatoria si arricchisce di una funzione ausiliaria rispetto alle attività dell'Ufficio, poiché l'univocità del sistema di catalogazione rende disponibile per via telematica tutta la documentazione di stampa collegata ai singoli provvedimenti.

Questo sistema di trasmissione *on line* potrà comodamente interfacciarsi con il sito *Web* del Garante costituendo un *iperlink* dei documenti ufficiali nonché del testo del Bollettino.

La creazione di un archivio telematico dei materiali va di pari passo con l'allargamento dei criteri di raccolta della documentazione. Nel progetto del Centro di documentazione rientra perciò l'apertura di una biblioteca di approfondimento del concetto di *privacy* in chiave interdisciplinare, con attenzione ai campi del diritto, della filosofia, della sociologia e della storia della tecnologia. La biblioteca - per la quale è prevedibile la progressiva disponibilità di ca. 4mila volumi e delle collezioni complete di circa 30 riviste italiane e straniere - sarà destinata anche a una utenza esterna qualificata di ricercatori e di studiosi interessati ad analizzare argomenti di rilevanza particolare.

Sempre nell'ambito delle iniziative del Centro di documentazione, l'editore Laterza è stato incaricato della pubblicazione dei *Quaderni del Garante*. I *Quaderni* avranno periodicità quadrimestrale (il n. 1 è attualmente in corso di stampa) e saranno aperti a collaboratori esterni. La loro finalità è quella di raccogliere contributi di provenienza diversa su singoli temi in modo da evidenziare il rapporto spesso di leggibilità non immediata ma anzi controverso e complesso tra la *privacy* e le nuove strutture della società dell'informazione.

3.2.10 Assetto organizzativo per il 1998

Nel 1998 l'Autorità si è avvalsa di un contingente di personale di 39 unità, poste in posizione di comando o fuori ruolo. Delle predette unità, l'80% circa riveste una qualifica direttiva (comprendendo in questa definizione il personale dalla VII alla IX qualifica funzionale), o dirigenziale.

L'Ufficio si è, altresì, avvalso di 12 consulenti, con la finalità precipua di approfondire le problematiche connesse con la realizzazione del sistema informativo e con la creazione del sito *Web* del Garante, nonché di acquisire esperienze e professionalità, nel campo giuridico e amministrativo, decisive soprattutto nella prima fase di vita dell'Ufficio stesso.

Al 31 dicembre 1998, le consulenze in atto erano 5.

Tabella 3 - Contingente di personale in servizio presso l'ufficio del Garante per la protezione dei dati personali e rapporti di consulenza avviati

Qualifica	Comando	Fuori ruolo	Consulenti
Dirigenti generali o equiparati		1	
Dirigenti o equiparati	1	5	
IX qualifica funzionale		3	
VIII qualifica funzionale		11	
VII qualifica funzionale	1	9	
VI qualifica funzionale		1	
V qualifica funzionale	1	4	
IV qualifica funzionale		1	
III qualifica funzionale		1	
Totale	3	36	12 (*)

Il personale in servizio presso l'Autorità proviene per la maggior parte dalle pubbliche amministrazioni; due unità appartengono ai ruoli delle magistrature ordinaria e contabile e uno al comparto degli enti di ricerca.

Quanto alla formazione, 30 unità su 39 sono in possesso di laurea, 8 di diploma di scuola media superiore e una di licenza media.

Tabella 4 - Personale per tipo di formazione ed esperienza lavorativa precedente

Esperienze precedenti	Laurea	Diploma sc. media sup.	Licenza media	Totale
Pubblica amministrazione	27	8	1	36
Magistratura amministrativa, ordinaria, contabile	2			2
Università o centri di ricerca	1			1
Totale	30	8	1	39

(*) 5 alla data del 31 dicembre 1998.

Dall'analisi per classi di età, emerge che il 50% del contingente si colloca nelle fasce centrali di età (comprese fra 30 e 39 anni), che un terzo del personale non supera i 34 anni, mentre solo 11 unità si collocano oltre i 45 anni di età. L'età media è di 39,7 anni.

Tabella 5 - Personale per classi di età

ANNI	< 30	30-34	35-39	40-45	45>
	2	9	11	5	11

3.2.11 Sede dell'Ufficio

Superata la fase di avvio dell'Ufficio, durante la quale la disponibilità di locali è stata garantita solo grazie alla collaborazione della Camera e del Senato, questa Autorità utilizza attualmente alcuni vani posti a disposizione dal Senato in Via della Chiesa Nuova, nonché un immobile di proprietà privata di circa 500 mq, per la cui locazione è stata acquisita l'autorizzazione dell'Ufficio del Programma per Roma Capitale.

Tali unità immobiliari sono da tempo assolutamente insufficienti per ospitare a regime, in maniera funzionale, l'intera struttura organica, per la cui collocazione si è rivelato necessario disporre di un immobile di almeno 2500 mq.

Dopo aver ricevuto la conferma dall'amministrazione finanziaria che non esistevano edifici demaniali o patrimoniali idonei all'uso richiesto e aver accertato che vari istituti ed enti previdenziali non possedevano immobili aventi le caratteristiche richieste, si è proseguita una attenta ricerca - già avviata dal maggio del 1997 - utilizzando tutti gli strumenti offerti dal mercato e cioè:

- contatti con altri enti e amministrazioni;
- esame di annunci economici pubblicati su riviste specializzate;
- indagine presso varie società immobiliari;
- pubblicazione di un avviso di ricerca di immobile su quotidiani.

La ricerca e la scelta sono state orientate in una zona centrale, considerata la necessità per questa Autorità di dislocare i propri uffici in un'area limitrofa a quella di vari altri organi istituzionali e amministrazioni che hanno frequenti contatti con l'Ufficio. La ricerca si è basata, come parametro decisivo, su quello di economicità e vantaggi per l'Ufficio, tenendo peraltro conto della necessità di usufruire di una sala convegni e di un'annessa biblioteca (che verrebbe messa a disposizione, mediante apposita convenzione, anche di altri organismi specie pubblici per iniziative di pubblico interesse), e di garantire un giusto decoro all'Ufficio che mantiene stretti contatti con altre autorità garanti straniere, ospitando anche rappresentanti stranieri in occasione di riunioni e seminari.

Le suddette ricerche di mercato e le offerte pervenute hanno consentito di individuare varie proposte immobiliari fra le quali, sulla base di un attento studio comparativo, è stata selezionata quella relativa ad alcune unità site nel «Palazzo Macchi di Celere» con accesso da Piazza di Montecitorio 115 - 121.

Sulla base del parere favorevole reso dall'Ufficio tecnico erariale di Roma (in merito alla congruità del canone di locazione richiesto), e dell'emanando decreto interministeriale per l'assenso alla locazione da parte dell'Ufficio Roma Capitale, si è potuto concludere un contratto preliminare il 31 dicembre 1998, approvato poi dal Garante in data 7 gennaio 1999.

È previsto un trasferimento graduale delle unità di personale nel corso del 1999 che dovrebbe essere ultimato, parallelamente ai lavori di sistemazione, entro il mese di febbraio del prossimo anno.

3.2.12 Dati sulle principali attività del Garante

I seguenti dati quantitativi si riferiscono al periodo 1° gennaio - 31 dicembre 1998.

Tabella 6 - Dati sulle principali attività del Garante

Attività	Numero
Richieste di informazione e quesiti telefonici	13.000
Segnalazioni, reclami, quesiti e prospettazioni di problemi applicativi	7.000
Assistenza telefonica relativa alle notificazioni	15/20.000
Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28 (dato aggiornato al 19/3/99)	270.000
Comunicazioni previste dall'art. 27, comma 2	346
Autorizzazioni al trattamento dei dati sensibili (art. 22) rilasciate per categorie di titolari e di trattamenti (art. 41, comma 7)	6
Autorizzazioni rilasciate a singoli destinatari	3
Risposte a richieste di autorizzazione (art. 22)	146
Comunicazioni in tema di dati sensibili e giudiziari previste dall'art. 41, comma 5	537
Segnalazioni del Garante	112
Provvedimenti di richiesta di informazioni e documenti (art. 31 e 32, comma 1)	950
Altri provvedimenti relativi a ricorsi (art. 29)	14
Risposte a quesiti formulati per iscritto	150
Pareri	70
Comunicati stampa e dichiarazioni alla stampa	61
Bollettini	4

3.2.13 Indagine conoscitiva

Ulteriori dati ed elementi relativi al Garante, alla natura delle sue attività, all'organizzazione dell'Ufficio, potranno essere forniti in occasione dell'indagine conoscitiva sulle autorità amministrative indipendenti, attualmente in corso di svolgimento presso la Camera dei Deputati.

Infatti, il 19 gennaio 1999, la I Commissione affari costituzionali ha deliberato di dar luogo a un'indagine per favorire una approfondita riflessione sulla posizione delle Autorità indipendenti nel sistema costituzionale, con specifico riferimento ai rapporti intercorrenti tra esse e gli altri poteri dello Stato.

Verranno così raccolti elementi di conoscenza relativi alle competenze, all'organizzazione interna, allo *status* delle Autorità, ai loro caratteri di autonomia e indipendenza, al fine di pervenire ad una razionalizzazione, all'individuazione di denominatori comuni, alla predisposizione di una disciplina legislativa unitaria.

Il Garante – così come le altre Autorità indipendenti – avrà modo di portare il proprio contributo in occasione delle audizioni che sono state previste nell'ambito dell'indagine conoscitiva.

4 ATTIVITÀ COMUNITARIE E INTERNAZIONALI

4.1 PREMESSA

Nel periodo considerato l'impegno del Garante per seguire le attività in corso a livello europeo e internazionale è cresciuto ulteriormente a causa dell'intensificarsi del carattere di «orizzontalità» che l'esigenza di una tutela adeguata dei dati personali assume riguardo alle iniziative tendenti a predisporre strumenti di coordinamento, anche normativo, delle azioni dei Governi e degli altri soggetti interessati allo sviluppo della Società dell'Informazione. La necessità di un bilanciamento degli interessi di volta in volta coinvolti si pone in maniera sempre più stringente, proprio per evitare il predominio delle esigenze del «mercato» e dei soggetti pubblici che trattano i dati su quelle dei consumatori e degli altri individui da tutelare.

È proseguita, inoltre, da parte del Garante l'opera di promozione della conoscenza negli altri Paesi della Comunità della normativa italiana che ha in buona misura attuato la direttiva 95/46/CE e la direttiva 97/66 sulla tutela della vita privata nel settore delle telecomunicazioni. Per entrambe il termine di recepimento era fissato al 24 ottobre 1998, ma allo stato attuale solo alcuni Stati membri hanno completato l'iter parlamentare per la trasposizione della prima direttiva e quattro quello della seconda direttiva (per un quadro comparativo delle singole legislazioni nazionali, si rinvia al successivo § 4.2.2.)

Altri importanti avvenimenti hanno caratterizzato l'attività del Garante per il 1998 per le notevoli implicazioni sotto il profilo della tutela dei dati personali: in particolare l'entrata in funzione dell'Ufficio europeo di Polizia (EUROPOL), avvenuta il 1° ottobre 1998 e la Conferenza ministeriale svoltasi a Ottawa, il 7-9 ottobre 1998, organizzata dall'OCSE sullo sviluppo del commercio elettronico.

Proprio il tema del commercio elettronico e dei modi per favorirne la diffusione a livello europeo e mondiale, salvaguardando o definendo i necessari livelli di tutela della riservatezza, è considerato oggi cruciale. Diverse sono le iniziative e le sedi che sono state individuate per aprire un confronto: oltre ai lavori già citati svolti in seno all'OCSE, occorre menzionare il completamento della lunga fase di elaborazione che ha portato il Consiglio d'Europa a predisporre «Linee-guida» sull'uso di Internet e ad approvare il 23 febbraio 1999 una «Raccomandazione» per consentirne la diffusione e l'applicazione. Il Garante, come già detto (v. cap. 2.13 e § 3.2.5), si è fatto promotore di un convegno internazionale, svoltosi a Roma nei giorni 8 e 9 maggio, proprio per riflettere e tenere conto delle diverse elaborazioni e soluzioni adottate dai diversi Paesi in relazione ai rapporti tra «Internet e privacy» (gli atti del convegno sono pubblicati a cura della Presidenza del Consiglio dei ministri, Dipartimento per l'informazione e l'editoria, Roma, 1999).

Le Comunità europee, attente agli sviluppi della Società dell'Informazione e dei riflessi sul mercato interno della globalizzazione dell'economia, hanno presentato poi due proposte di direttive, rivolte ad armonizzare l'una il quadro legale per l'utilizzo della firma elettronica, l'altra alcuni aspetti giuridici del commercio elettronico. Le proposte sono entrambe in discussione nei gruppi di lavoro del Consiglio.

Altro importante settore di attenzione, ancorché ancora non completamente definito nelle sue concrete implicazioni, riguarda l'entrata in vigore del Trattato di Amsterdam e la definizione del cd. *acquis* di Schengen.

4.2 NORMATIVA COMUNITARIA

4.2.1 La direttiva-quadro n. 95/46/CE e la direttiva n. 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni

Gli aspetti relativi alla tutela dei dati personali sono affrontati, come già indicato nella *Relazione per l'anno 1997*, dal «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali» (organismo a carattere consultivo e indipendente composto dai rappresentanti delle Autorità di controllo nazionali e istituito dall'art. 29 della direttiva) e da un Comitato previsto dall'art. 31 della stessa (che assiste la Commissione ed esprime il suo parere su progetti da essa sottoposti).

La vicepresidenza del Gruppo è affidata al Presidente del Garante, prof. Stefano Rodotà, che ha presieduto la riunione del 25 gennaio 1999.

Il Gruppo ha adottato, in particolare, i seguenti atti (v. *Allegati*, cap. 5.7):

- Raccomandazione 1/98, adottata il 28 aprile 1998, in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo;
- Parere 1/98, adottato il 16 giugno 1998, sulla piattaforma per le preferenze in materia di protezione della vita privata (P3P- Platform for Privacy Preferences) e la «norma aperta per i profili» (OPS-Open Profiling Standard);
- Documento di lavoro sul trasferimento dei dati personali verso Paesi terzi approvato il 24 luglio 1998: applicazione degli artt. 25 e 26 della direttiva europea sulla tutela dei dati;
- Documento sull'attività futura riguardante i codici di condotta, con particolare riferimento alla definizione della procedura relativa alla valutazione dei codici di condotta comunitari a opera del Gruppo, approvato il 10 settembre 1998;
- Parere 1/99 relativo al livello di protezione dei dati negli Stati Uniti e al dibattito in corso fra la Commissione europea e il Governo degli Stati Uniti, adottato il 26 gennaio 1999.

Il termine del 24 ottobre per il recepimento è scaduto e, come già anticipato, solo una parte dei Paesi ha provveduto alla trasposizione. Anche l'Italia non ha ultimato la trasposizione della direttiva e dovrà pertanto completare l'iter con sollecitudine, utilizzando lo strumento dei decreti delegati che possono essere adottati entro il 31 luglio 1999.

Peraltro, secondo un orientamento informale della Commissione europea che si basa sulla più generale giurisprudenza elaborata dalla Corte di giustizia delle Comunità europee, la direttiva sarebbe direttamente applicabile per taluni aspetti in virtù dell'effetto verticale diretto, attribuito ad alcune parti chiaramente e immediatamente dispositive.

Da quanto emerso nelle riunioni dei gruppi di lavoro, le difficoltà maggiori dei Paesi Ue sembrano legate alla soluzione di aspetti relativi al trasferimento dei dati da e verso Paesi terzi (artt. 25 e 26 della direttiva), nonché alla determinazione della legge applicabile, alla nozione di stabilimento (art. 4 della direttiva), al «bilanciamento degli interessi» secondo l'art. 7, lett. b), al cd. *prior-checking* (art. 20 della direttiva) e alla natura e all'adequatezza delle sanzioni. Il Garante ha pertanto proposto ai rappresentanti delle autorità di controllo che compongono il Gruppo di riflettere e confrontare le proprie esperienze. Dopo ampia valutazione, il Gruppo ha stabilito alcune priorità di azione che comporteranno approfondimenti da curare anche attraverso un seminario di lavoro in Italia.

Il Gruppo si è anche occupato della definizione del regolamento che dovrà portare alla istituzione di un organo di controllo indipendente, incaricato, secondo l'art. 286 del Trattato di Amsterdam, di sorvegliare l'applicazione degli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali - in sostanza le direttive citate - alle istituzioni e agli organismi comunitari. Tale autorità avrebbe dovuto essere già operante alla data del 1° gennaio 1999, ma i ritardi nella ratifica del Trattato di Amsterdam da parte di alcuni Paesi dell'Unione ne hanno finora impedito l'entrata in vigore.

Anche le istituzioni comunitarie, quindi, saranno tra breve chiamate ad applicare pienamente al loro interno i principi delle direttive, incaricando un apposito organismo di svolgere un controllo indipendente sul loro rispetto.

A seguito dell'entrata in vigore della direttiva 97/66/CE del 15 dicembre 1997, il cui termine di recepimento, come si è detto, era fissato anch'esso al 24 ottobre 1998 (e che è stata attuata dall'Italia con il decreto n. 171 del 13 maggio 1998) il Gruppo ha visto estendere i suoi compiti «alla tutela dei diritti e delle libertà fondamentali, nonché dei legittimi interessi nel settore delle telecomunicazioni», ai sensi dell'art. 14, § 3 della direttiva.

Il Comitato previsto dall'art. 31, nell'imminenza dell'entrata in vigore della direttiva, ha invece incentrato i suoi lavori soprattutto sugli aspetti legati alla definizione del concetto di adeguatezza ai fini del trasferimento di dati verso Paesi terzi. Particolare delicatezza ha assunto a questo riguardo il dialogo con gli Stati Uniti, considerando le diversità esistenti tra le due parti nel considerare questo tema. Numerosi sono stati i colloqui e gli incontri, tra cui assume indubbio rilievo la visita effettuata in Italia il 26 gennaio 1999 dal Sottosegretario al commercio estero americano, ambasciatore Aaron, e l'incontro con il Garante avutosi nell'occasione.

Altri temi di interesse attengono ai lavori del gruppo di lavoro «problemi economici - protezione dati» del Consiglio: nel corso dell'anno l'attenzione è stata posta sulla definizione dei modi per consentire l'adesione delle Comunità europee alla Convenzione n. 108 del Consiglio d'Europa e alla connessa posizione comunitaria, espressa attraverso la Commissione riguardo al progetto di «Linee-guida» su Internet e, soprattutto, al protocollo aggiuntivo alla Convenzione n. 108 con il quale si intendono apportare alla stessa importanti modificazioni per renderla più in linea con il contenuto della direttiva 95/46/CE. Il protocollo disciplina la creazione di autorità di controllo nazionali e la trasmissione di dati verso Paesi terzi.

Altro importante tema che ha caratterizzato i lavori del Gruppo, soprattutto nella prima metà dell'anno, è stato quello della definizione della posizione dei quindici Paesi dell'Unione in relazione al progetto di dichiarazione dei ministri partecipanti alla conferenza di Ottawa sul commercio elettronico relativa alla tutela della *privacy*.

La Commissione europea ha infatti partecipato ai lavori preparatori in seno all'OCSE, rappresentando, di volta in volta il punto di vista dell'Ue rispetto ai testi proposti.

4.2.2 Quadro comparativo sul recepimento delle direttive 95/46/CE e 97/66/CE nei Paesi membri dell'Ue

L'elemento caratterizzante il 1998 in chiave di normativa sovranazionale applicabile ai dati personali è stata la scadenza del termine di recepimento della direttiva 95/46 al giorno 24 ottobre. Alla stessa data era prevista anche l'analoga scadenza

per un'altra direttiva strettamente legata alla precedente (tanto da essere detta comunemente «direttiva-figlia»), ossia la 97/66 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni.

Le posizioni dei singoli Stati appartenenti all'Unione europea possono quindi essere utilmente collocate in rapporto a tale scadenza, nel senso che non tutti hanno recepito in tempo le disposizioni comunitarie attraverso la legislazione nazionale. Possiamo dunque esaminare in prima battuta gli sviluppi legati alla direttiva «madre»; vedremo successivamente il quadro legislativo nazionale per quanto riguarda la direttiva «figlia».

In particolare, tre Stati (*Portogallo* - Lei da Protecção de Dados Pessoais no. 67/98; *Regno Unito* - Data Protection Act (DPA) of 16th July 1998; *Svezia* - Personuppgiftslag ov 29 april 1998) hanno completato per primi i lavori parlamentari per il recepimento della direttiva 95/46 entro il termine previsto, e in un quarto (il *Belgio* - Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) il Parlamento ha licenziato il testo definitivo della nuova legge nel mese di dicembre 1998. Essi si sono così aggiunti all'Italia e alla Grecia, che avevano già recepito in gran parte la normativa comunitaria rispettivamente attraverso la l. n. 675/1996 e la l. n. 2472/1997.

È bene premettere che tutti e quattro i Paesi citati disponevano già di leggi in materia di protezione dei dati e di autorità incaricate di vigilare su tale protezione. Il recepimento della direttiva comunitaria ha quindi comportato un adeguamento della legislazione preesistente attraverso integrazioni o modifiche delle disposizioni già in vigore.

Le leggi nazionali di recepimento in linea di massima presentano forti analogie in termini sia di struttura sia di contenuti. I principi fondamentali della direttiva trovano ovviamente tutti attuazione, a partire dai diritti dell'interessato (accesso, opposizione, informazione) fino all'obbligo di notifica preventiva del trattamento a una Autorità indipendente, al divieto di trasferire dati verso Paesi terzi tranne in casi determinati, alla definizione dei compiti e dei poteri dell'Autorità di controllo, alle sanzioni previste per le inadempienze. Tuttavia, i legislatori dei singoli Paesi hanno fatto uso del margine di manovra loro riconosciuto nell'attuazione delle disposizioni comunitarie, per cui esistono alcune significative differenze fra le varie leggi che sarà interessante evidenziare, anche in rapporto alla scelta operata dal legislatore italiano.

Tutti e quattro i testi approvati nel corso del 1998 prevedono che il trattamento dei dati personali possa avvenire solo con il consenso dell'interessato o in base ad altri precisi presupposti, in ciò uniformandosi al principio sancito dagli artt. 7 e 8 della direttiva. Mentre però la legge belga distingue fra dati personali (art. 5), per i quali occorre che l'interessato abbia «indubitablement donné son consentement» e dati «sensibili» (art. 6), per i quali occorre il consenso «par écrit», negli altri testi non si fa menzione di un consenso «per iscritto» - uniformandosi al dettato degli artt. 7 e 8 della direttiva. La legge inglese, ad esempio, parla di «explicit consent» nel caso dei dati sensibili, mentre usa il solo termine «consent» per i dati personali in genere.

Considerazioni analoghe valgono per la legge portoghese, ove si parla di «consentimento expresso» e di «consentimento», rispettivamente. Si realizza dunque un livello diverso di tutela non sempre del tutto omogeneo rispetto a quanto previsto dal legislatore italiano, che ha scelto di introdurre una garanzia ulteriore ai fini della manifestazione della libera volontà degli interessati.

Anche per quanto riguarda l'informativa all'interessato le indicazioni della direttiva sono recepite nel dettaglio in rapporto all'obbligo di indicare l'identità del responsabile del trattamento e le finalità di quest'ultimo, fornendo per il resto indicazioni puramente esemplificative («any further information which is necessary», DPA, Schedule I, Part II, 2(3); «outras informacoes, tais como: (?)», Lei 67/98, Art. 10(1); «all övrig information», Personuppgiftslag art. 25). La legge belga menziona invece esplicitamente anche il diritto di opposizione dell'interessato fra le informazioni da fornire a quest'ultimo.

La direttiva riconosce alcune esenzioni per quanto riguarda gli obblighi di informativa degli interessati, in particolare rispetto ai trattamenti per scopi di pubblica sicurezza e per finalità di giornalismo o espressione artistica o letteraria. Le legislazioni nazionali hanno recepito tali esenzioni, seppure in modo non uniforme. Ad esempio, la legge inglese (DPA) prevede in una apposita sezione esenzioni più o meno ampie a seconda che i dati attengano alla salvaguardia della sicurezza nazionale (con una deroga a principi di legittimità, adeguatezza, pertinenza, esattezza, ecc.), alla prevenzione e repressione di reati (limiti al principio di liceità e correttezza e ai diritti di accesso dell'interessato) o ai dati trattati nell'ambito di finalità giornalistiche o sanitarie o di ricerca storica e statistica (artt. 27-33).

La legge portoghese afferma chiaramente l'applicabilità delle disposizioni della legge stessa ai dati il cui trattamento sia finalizzato alla sicurezza pubblica, la difesa nazionale e la sicurezza dello Stato (art. 4(7)), ma è previsto che si possa fare riferimento a norme di legge specifiche. La dispensa dall'obbligo dell'informativa è esplicitamente prevista, oltre che in questi casi, per i trattamenti di natura giornalistica (art. 10(5) e 10(6)). Come si vede, si tratta di una materia che deve essere ulteriormente precisata attraverso la legislazione secondaria. Quest'ultima esigenza viene esplicitamente richiamata anche nella legge belga in rapporto ai trattamenti effettuati dal «Centre européen pour enfants disparus et sexuellement exploités» istituito nel 1997.

Anche in tema di notificazione del trattamento, pur prevedendosi in tutti i casi l'obbligo di notificare i trattamenti di dati personali (con determinate eccezioni) e di istituire un registro dei trattamenti, esistono alcune differenze nelle modalità specifiche di attuazione. Ad esempio, il DPA prevede che la notificazione effettuata sia mantenuta nel registro per un periodo determinato (di regola non superiore a un anno) e venga poi cancellata in mancanza del pagamento della prescritta tassa (art. 19 DPA).

Per quanto riguarda le esenzioni, la legge portoghese demanda all'Autorità nazionale di controllo il compito di autorizzare notificazioni in forma semplificata o esenzioni tramite provvedimenti da pubblicare sul *Diário da República*, mentre nel caso del Belgio è un'ordinanza reale, sentito il parere dell'Autorità nazionale di controllo, a stabilire i casi nei quali la notificazione può essere presentata in forma semplificata o può non essere presentata.

In tutti i casi il criterio-guida comune è quello enunciato nell'art. 18 (2) della direttiva e ripreso in modo letterale nei singoli testi di legge, ossia che si tratti di categorie di trattamento che non rechino pregiudizio ai diritti e alle libertà della persona interessata. Anche in questo campo occorrerà dunque attendere l'intervento di normative secondarie che daranno effettiva attuazione alle disposizioni della legge di recepimento.

Un altro ambito di rilevante interesse è rappresentato dalle norme che regolano il trasferimento di dati personali verso Paesi terzi. Il tema è particolarmente delicato, ed è oggetto di numerose riflessioni e discussioni a livello Comunitario che vertono, in modo particolare, sui criteri per valutare l'«adeguatezza» del livello di protezione

offerto nel Paese terzo (v. cap. 2.13). I legislatori nazionali hanno recepito il testo della direttiva in modo pressoché letterale, adottando il criterio dell'adeguatezza quale requisito per il trasferimento. È interessante osservare, inoltre, che in varie leggi nazionali si fa esplicito riferimento all'esistenza nel Paese terzo di codici di condotta quale circostanza da prendere in esame nel valutare l'adeguatezza del livello di protezione.

Peraltro, nel DPA si prevede che i Paesi terzi non sono i Paesi non appartenenti all'Ue, bensì quelli che non appartengono allo Spazio economico europeo così come definito dall'accordo di Oporto del 1992. In pratica, oltre ai Paesi dell'Ue, è ammesso il trasferimento di dati verso i Paesi membri della CECA, la Svizzera, il Liechtenstein, l'Islanda e la Norvegia. Un'analoga disposizione è contenuta anche nel Personuppgiftslag svedese.

Per completare il quadro relativo all'Ue è bene fare un cenno alla situazione del processo legislativo negli altri Paesi, che fino al febbraio 1999 non avevano ancora recepito la direttiva 95/46. Va detto che in tutti erano già precedentemente in vigore leggi relative alla protezione dei dati personali; tuttavia, mentre alcuni (Austria, Danimarca, Paesi Bassi e Spagna) hanno già elaborato disegni di legge che prevedono emendamenti alla legislazione esistente in rapporto alle indicazioni della direttiva, i restanti (Francia, Germania, Irlanda e Lussemburgo) stanno provvedendo in tal senso - per motivazioni di varia natura legate alla complessità della materia, alla difficoltà delle scelte e, in taluni casi, a riserve e resistenze emerse.

In Francia - ove peraltro esiste una legge che dal 1978 disciplina la materia e ha istituito la *Commission Nationale de l'Informatique et des Libertés* - non è stato ancora elaborato un disegno di legge anche se il Governo intende muoversi con rapidità sulla base del dibattito stimolato dal «rapporto Braibant». Per quanto riguarda la Germania, il Governo dovrà ripresentare un disegno di legge dopo che il precedente (dell'8 aprile 1998) non è stato oggetto di esame a causa delle elezioni tenutesi il 27 settembre 1998. Anche in Irlanda e Lussemburgo il Governo deve tuttora presentare un disegno di legge. In Finlandia, invece, la legge approvata di recente entrerà in vigore il 1° aprile 1999.

Strettamente connessa alla direttiva 95/46 è l'altra direttiva cosiddetta «figlia» (97/66 del 15 dicembre 1997) che, come si è detto, è entrata in vigore egualmente il 24 ottobre 1998. La direttiva è finalizzata ad armonizzare le disposizioni degli Stati membri per garantire un livello «equivalente» di tutela dei diritti e delle libertà fondamentali, «ed in particolare del diritto alla vita privata», rispetto al trattamento di dati personali nel settore delle telecomunicazioni (art. 1, comma 1).

Di fatto, come stabilito dal comma 2 dell'art. 1, le disposizioni di questa direttiva «precisano e integrano la direttiva 95/46/CE» - tanto che vengono riprese le stesse definizioni contenute nell'art. 2 della direttiva «madre» con l'aggiunta di alcune specificamente riferite al settore delle telecomunicazioni (abbonato, utente, rete pubblica di telecomunicazione, servizio di telecomunicazione).

La direttiva indica in sostanza le modalità atte a garantire i principi sanciti nella 95/46 rispetto ai servizi offerti sulle reti pubbliche di telecomunicazioni, anche con riguardo alle persone giuridiche. Esse sono relative ai seguenti temi:

- sicurezza del trattamento;
- riservatezza delle comunicazioni (divieto di intercettazione senza consenso, tranne che per gli scopi indicati all'art. 14 - v. qui di seguito);
- conservazione dei dati solo per scopi determinati e non oltre il periodo necessario;

- diritto degli abbonati all'informazione sulla linea chiamante e collegata (o alla soppressione di tali informazioni);
- diritto alla cancellazione (parziale o totale) dei propri dati contenuti in elenchi degli abbonati a disposizione del pubblico;
- necessità del consenso dell'abbonato per l'invio di chiamate a scopi pubblicitari.

La direttiva prevede inoltre (art. 14) l'estensione del campo di applicazione di alcune disposizioni della direttiva 95/46; in particolare, ciò si applica alla limitazione degli obblighi sopra indicati per finalità di sicurezza dello Stato, difesa, pubblica sicurezza, prevenzione, ricerca, accertamento e perseguimento di reati.

Si tratta, come si vede, di una serie di obblighi ai quali gli Stati membri sono chiamati a far fronte attraverso disposizioni legislative, regolamentari e amministrative che incidono su settori particolarmente delicati: basti pensare, ad esempio, alla fornitura di servizi via Internet. È quest'ultimo punto, in effetti, ad avere suscitato le maggiori perplessità e incertezze, che l'Italia ha risolto (seppure in parte) attraverso il d.lg. n. 171 del 13 maggio 1998 (v. § 2.12.1).

Le stesse perplessità e incertezze hanno caratterizzato il recepimento della normativa comunitaria negli altri Stati membri, cosicché alla data prevista per l'entrata in vigore della direttiva soltanto quattro Paesi, oltre all'Italia, avevano provveduto a emanare disposizioni nazionali per la trasposizione della direttiva (Austria, Germania, Finlandia, Portogallo). Un progetto di legge è stato presentato nel Regno Unito.

4.2.3 Lo sviluppo della Società dell'Informazione e l'attività della Commissione europea: le proposte di direttiva relative a un quadro comune sulle firme elettroniche e all'armonizzazione di alcuni aspetti del commercio elettronico

La proposta di direttiva relativa a un quadro comune sulle firme elettroniche, presentata dalla Commissione il 22 giugno 1998, doc. COM (98) 0297, è finalizzata a introdurre una cornice di regole armonizzate tra i Paesi membri delle Comunità europee per l'utilizzo delle firme elettroniche. L'intervento è stato ritenuto necessario per favorire lo sviluppo del commercio elettronico e si riferisce principalmente, anche se non esclusivamente, alle transazioni tra privati.

La direttiva prende infatti in considerazione anche l'uso delle firme elettroniche nei rapporti con la pubblica amministrazione o, meglio, con il settore pubblico. Essa, inoltre, detta regole per garantire il riconoscimento giuridico delle firme elettroniche, stabilendone l'equiparazione a quelle autografe. Il principio cardine della direttiva consiste nell'evitare qualsiasi forma di discriminazione delle firme elettroniche sulla sola base dell'essere le firme stesse sotto forma elettronica, assicurando, in presenza di precisi requisiti di sicurezza, che esse siano considerate come pienamente equivalenti alle firme apposte manualmente.

I principi su cui si basa la direttiva sono quelli della neutralità tecnologica, evitando di legare la direttiva a uno o più prodotti in commercio e tenendo conto del rapido evolversi delle tecnologie e della libertà d'impresa. È pertanto escluso che gli Stati possano introdurre o mantenere regimi di autorizzazione preventiva, mentre hanno facoltà di mantenere o introdurre regimi di «accreditamento» facoltativi per garantire un più alto livello di sicurezza e affidabilità dei prestatori di servizi di certificazione e dei certificati da questi emessi.

Particolare importanza riveste per il Garante, che partecipa alle riunioni del gruppo di lavoro a Bruxelles, la parte relativa alla protezione dei dati personali, all'uso dello pseudonimo, agli aspetti transfrontalieri, alla definizione delle responsabilità dei prestatori di servizi di certificazione e alla individuazione degli specifici requisiti, tecnici e professionali, che gli stessi debbono possedere. Il testo inizialmente proposto dalla Commissione è stato largamente modificato nel corso delle riunioni ed è stato presentato al Consiglio dei ministri delle telecomunicazioni dell'Unione europea il 27 novembre per un accordo di massima; successivamente ripreso dal gruppo di lavoro, è stato ulteriormente e profondamente modificato sia nella parte relativa alla definizioni, ove sono stati introdotti riferimenti alle firme elettroniche avanzate e ai dispositivi «sicuri» di creazione e verifica delle firme stesse sia, soprattutto, in una più chiara identificazione degli elementi necessari per poter fondare una presunzione di equivalenza con le firme manoscritte.

Nel novembre 1998 è stata presentata dalla Commissione la proposta di direttiva del Parlamento europeo e del Consiglio COM (1998) 586 def. relativa a taluni aspetti del commercio elettronico nel mercato interno. Si tratta di una proposta di tipo orizzontale, in quanto si aggiunge alle direttive che già disciplinano i diversi settori interessati, dettando delle norme solo per la parte che rileva ai fini del commercio elettronico. La proposta - che intende armonizzare il quadro di riferimento, in particolare rispetto a cinque aspetti ritenuti cruciali, per evitare che gli Stati membri adottino in materia legislazioni divergenti, creando ostacoli e turbative al mercato interno - ha destato sia nelle riunioni di coordinamento interministeriali sia in seno al gruppo di lavoro del Consiglio che la sta discutendo, diverse perplessità. Gli aspetti che la direttiva intende armonizzare riguardano:

- la definizione del luogo di stabilimento dei fornitori di servizi della Società dell'Informazione;
- la definizione della nozione di comunicazione commerciale e misure per incoraggiarne l'uso;
- la stipulazione di contratti *on-line* (collegata all'approvazione della proposta di direttiva sulle firme elettroniche);
- la definizione di principi comuni di responsabilità per i fornitori di servizi *on-line*;
- la previsione di sistemi volti a favorire l'effettiva attuazione delle norme comunitarie.

La proposta si presenta poi di difficile lettura per i molteplici richiami e rinvii operati ad altre direttive, nonché per le esclusioni e deroghe ivi previste.

Il Garante è interessato più direttamente alle parti che attengono alla tutela dei dati personali, per i quali si ritiene del tutto insoddisfacente la clausola di esclusione approntata dall'art. 22. Infatti accanto alla estrema specificità delle previsioni della direttiva, questo articolo, intitolato «Deroghe», si limita a prevedere che la direttiva non si applica «alle materie regolate dalla direttiva 95/46/CE» e, quindi, risulta del tutto inadeguato per tenere conto di una disciplina che intende garantire una tutela generale.

La disciplina del rapporto tra il commercio elettronico e la tutela dei dati personali, se demandata a una mera clausola di deroga apposta in calce a una direttiva (quella sul commercio elettronico) che però reca disposizioni non sempre convergenti con quelle in materia di dati personali, potrebbe infatti ingenerare serie difficoltà in sede applicativa.

4.3 LA COOPERAZIONE EUROPEA NEI SETTORI GIUSTIZIA E AFFARI INTERNI

4.3.1 Consiglio giustizia e affari interni (Trattato di Amsterdam e proposta italiana per una omogeneizzazione)

Come già evidenziato nella precedente relazione, l'esistenza, nell'ambito del titolo VI del trattato di Maastricht, dedicato alla cooperazione in materia di affari interni e giustizia, di diversi strumenti basati su scambi informatizzati di dati personali, ha fatto ritenere opportuno, anche ai fini degli sviluppi derivanti dall'imminente entrata in vigore del nuovo Trattato, aprire una riflessione tendente a valutare l'opportunità di una razionalizzazione di quanto sinora realizzato o in via di realizzazione, soprattutto riguardo ai sistemi di tutela previsti, alle disposizioni in materia di responsabilità, ai compiti degli organi di supervisione e controllo.

Su proposta del Ministro dell'interno italiano, il Consiglio dei Ministri europei della giustizia e affari interni ha deciso di far effettuare una ricognizione puntuale dei diversi strumenti esistenti e in corso di definizione, di studiare le forme più idonee per ridurre le disarmonie esistenti nei diversi testi e il rischio di disparità di trattamento nel riconoscimento agli interessati dei diritti previsti in materia di protezione dei dati, e di razionalizzare la complessa tematica pervenendo a un grado più elevato di armonizzazione ed evitando duplicazioni di personale e mezzi. La ricognizione, curata dal servizio giuridico, e presentata in un documento dello scorso settembre, contiene anche interessanti riflessioni e specifici orientamenti.

Di conseguenza è stato deciso di dare uno specifico mandato a un gruppo di lavoro per proseguire la riflessione e presentare soluzioni.

La prima riunione del Gruppo ha avuto luogo l'11 febbraio 1999.

4.3.2 Schengen

Nel 1998 è proseguita l'opera di controllo svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'informazione di Schengen, anche attraverso le segnalazioni pervenute da privati.

Con i propri rappresentanti dell'Autorità comune di controllo istituita ai sensi dell'art. 115 della Convenzione di applicazione dell'Accordo di Schengen, il Garante ha contribuito poi all'adozione di specifiche raccomandazioni e pareri.

Si allega alla presente relazione il Rapporto dell'ACC relativo al periodo marzo 1997-marzo 1998. Si differisce invece la pubblicazione di quello relativo al periodo marzo 1998-marzo 1999 la cui predisposizione è ancora in corso.

Di particolare interesse la relazione dell'ACC relativa alla sicurezza degli uffici SIRENE (scaturita da una acquisizione illecita di dati verificatasi in un ufficio SIRENE, cui avevano fatto seguito ispezioni e verifiche da parte delle autorità nazionali per verificare le misure di sicurezza adottate in tutti gli uffici dei Paesi membri), datata 11 dicembre 1998 e presentata dall'ACC al Comitato esecutivo;

Sono stati adottati i seguenti pareri:

- 98/1 sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione nel SIS;

- 98/2 relativo alla segnalazione nel SIS di persone la cui identità è stata usurpata, il Protocollo per le visite e i controlli presso il C.SIS definito con le autorità francesi e l'ACC, definito dal Comitato di orientamento SIS nel dicembre scorso;

– 98/3 sulle eventuali relazioni tra il SIS e il progetto ASF (*automated search facility*) di INTERPOL;

– 98/4 relativo alle registrazioni delle consultazioni di cui all'articolo 103 della Convenzione.

Tema di grande attualità è quello dell'imminente trasposizione del quadro normativo fissato dagli Accordi di Schengen all'interno del sistema di integrazione europeo fissato dal Trattato di Amsterdam: quest'ultimo prevede infatti, in uno specifico protocollo, che l'*acquis* di Schengen sia integrato nell'ambito dell'Unione europea a decorrere dall'entrata in vigore, prevista per il prossimo mese di maggio.

Entro quella data quindi le attività, l'organizzazione, le strutture e i mezzi finanziari dedicati alla cooperazione Schengen dovranno trovare una collocazione all'interno delle corrispondenti strutture delle Comunità e dell'Unione in relazione alla base giuridica che sarà identificata come idonea per collocare e proseguire le suddette attività.

Delicati problemi si pongono, con riguardo alla struttura e al funzionamento del SIS, alla collocazione dell'ACC e, più in generale, alla identificazione di idonee soluzioni per garantire il sistema di tutela dei dati personali delineato.

Il tema è stato da ultimo evidenziato nell'audizione di un componente dell'Autorità avanti il Comitato parlamentare di controllo Schengen, svoltasi il 23 febbraio 1999.

Va segnalato infine che con l. 18 febbraio 1999, n. 47, è stato ratificato il protocollo recante modifica degli articoli 40, 41 e 65 della convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985, firmata a Schengen il 19 giugno 1990, fatto a Lisbona il 24 giugno 1997.

A seguito poi della deliberazione del'ACC di curare la pubblicazione di un opuscolo illustrativo delle modalità per esercitare il diritto di accesso ai dati detenuti nel Sistema informativo Schengen da parte dei soggetti interessati, è stato definito il testo e l'immagine della campagna informativa, che dovrà svolgersi nei vari Paesi Schengen secondo modalità uniformi. Al riguardo il Garante, che figura come l'autorità nazionale cui gli interessati potranno rivolgersi per gli accertamenti da svolgere in Italia, definirà in tempi brevi la stampa e la distribuzione degli opuscoli e dei pannelli informativi, anche attraverso l'eventuale collaborazione, finanziaria od organizzativa, di altre amministrazioni interessate.

4.3.3 Europol

La l. 23 marzo 1998, n. 93, ha autorizzato la ratifica e l'esecuzione della Convenzione basata sull'art. K3 del Trattato sull'Unione europea del 25 luglio 1995, che istituisce un Ufficio europeo di polizia (Europol). La stessa legge ha affidato al Garante per la protezione dei dati personali il ruolo di Autorità di controllo nazionale ai sensi dell'art. 23 della convenzione stessa.

Spetta quindi al Garante accertare che l'introduzione, la consultazione, la trasmissione, in qualsiasi forma, all'Europol di dati personali da parte dell'Italia avvengano nel rispetto delle norme; a tale fine il Garante avrà accesso ai dati e agli archivi. Sulla base dei principi dettati nelle ll. nn. 675/1996 e 676/1996, il Garante dovrà inoltre controllare le attività svolte dall'unità nazionale e dagli ufficiali di collegamento per la parte concernente le tutela dei dati personali. In base al disposto della Convenzione, che ha attribuito a chiunque il diritto di chiedere all'autorità di controllo nazionale di verificare la legittimità dell'introduzione e della trasmissione all'Europol di dati che lo riguardano, al Garante spetta inoltre di provvedere sulle specifiche istanze, nel rispetto delle procedure previste dalla l. n. 675/1996.

L'entrata in vigore della Convenzione al 1° ottobre 1998 ha determinato altresì l'inizio della funzionalità dell'Autorità comune di controllo prevista dall'art. 24 della Convenzione: questa Autorità, composta di due rappresentanti per Paese delle autorità nazionali di controllo, esercita controlli incisivi sulla gestione degli archivi Europol, decidendo anche sulle questioni sottoposte a mezzo di specifici ricorsi, esaminati in apposita composizione ristretta - dal comitato per i ricorsi -.

L'Autorità ha definito in un regolamento interno le necessarie misure procedurali e i compiti della struttura, attualmente al vaglio del Consiglio dei ministri degli affari interni e della giustizia, organo al quale spetta l'approvazione definitiva.

Tra gli atti necessari a consentire la piena operatività della Convenzione vi è il protocollo relativo ai privilegi e immunità di Europol: il disegno di legge italiano di ratifica non ha tuttora completato il suo *iter*, essendosi ritenuto necessario, come anche fatto presente dal Garante (in particolare nel corso di una audizione in Parlamento del Presidente del Garante), approfondire gli aspetti relativi alle garanzie riconosciute a Europol e ai suoi agenti e rappresentanti. Il protocollo conferisce infatti a Europol (art. 2, comma 1) l'immunità giurisdizionale per la responsabilità di cui all'art. 38, § 1 della Convenzione, rispetto al trattamento di dati illecito o effettuato in modo non corretto, disposizione che sembra introdurre una deroga alla normativa internazionale della protezione dei dati che ingenera il timore di una attenuazione delle garanzie contenute nella Convenzione. È stata pertanto fatta presente la necessità di avviare una consultazione, unitamente ai *partner* europei, riguardo all'opportunità di adottare misure idonee ad assicurare che in nessun modo l'attuazione delle disposizioni del Protocollo sui privilegi e le immunità di Europol possa determinare una diminuzione del livello di tutela offerto dalla Convenzione.

4.3.4 Sistema informativo doganale

Con la l. 30 luglio 1998, n. 291, l'Italia ha autorizzato la ratifica e l'esecuzione della Convenzione sull'uso dell'informatica nel settore doganale, elaborata in base all'articolo K3 del Trattato sull'Unione europea del 26 luglio 1995.

La Convenzione mira a intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Unione europea, particolarmente attraverso lo scambio di dati personali.

A tal fine è stata prevista la creazione di un sistema informativo automatizzato comune (Sistema informativo doganale, o SID) che dovrebbe facilitare la prevenzione, la ricerca e il perseguimento delle infrazioni alle leggi nazionali.

Nella legge di ratifica, a differenza delle scelte operate per la Convenzione Europol, non sono state introdotte disposizioni per individuare espressamente nel Garante l'Autorità nazionale di controllo, né le disposizioni specificamente applicabili.

Al riguardo sembra quindi opportuno il riferimento alla normativa esistente, secondo la quale il quadro interno di protezione dei dati sarà definito con i decreti delegati previsti dalla l. n. 676/1996, mentre la tutela nei confronti di trattamenti illeciti o irregolari sarà assicurata, a livello nazionale, dal Garante, in base alle procedure definite dalla l. n. 675/1996. Il Garante concorrerà poi, analogamente a quanto avviene per le altre Convenzioni di terzo pilastro che istituiscono sistemi informatizzati di raccolta e scambio di dati personali, alla composizione dell'Autorità comune di controllo, che in questa convenzione ha compiti prevalentemente di esame delle problematiche relative alla funzionalità del sistema di tutela previsto dalla Convenzione.

La Convenzione dovrebbe entrare in vigore al completamento delle procedure di ratifica nei vari Paesi, approssimativamente non prima dell'autunno del 1999.

4.3.5 Eurodac

Il progetto di Convenzione per l'istituzione di un sistema per la raccolta, la memorizzazione, il confronto e lo scambio di dati relativi alle impronte digitali dei richiedenti asilo, basata sull'art. 15 della Convenzione di Dublino relativa alla determinazione dello Stato competente per l'esame delle richieste d'asilo, prosegue i lavori nell'ambito dell'apposito gruppo.

Anche questo progetto di Convenzione rientra nella riflessione generale sull'opportunità di razionalizzare gli strumenti elaborati o in via di elaborazione nel settore della cooperazione affari interni e giustizia proposta dall'Italia.

4.4 CONSIGLIO D'EUROPA

Il Consiglio d'Europa ha proseguito la sua attività di elaborazione e sviluppo della normativa europea in materia di tutela dei dati personali, in particolare attraverso i lavori dei comitati plenari T-PD e CJ-PD e del gruppo GT-15.

Il Comitato consultivo della Convenzione n. 108 - T-PD, nella riunione annuale svoltasi all'inizio del mese di settembre, si è occupato prevalentemente della definizione dei modi per permettere l'adesione delle Comunità europee alla Convenzione. La decisione adottata è nel senso di emendarne il testo seguendo la procedura ordinaria prevista dall'art. 21, in quanto questa risulta più flessibile e rapida.

Le modifiche consistono nell'inserimento del riferimento alle Comunità europee accanto a quello agli Stati e alla modifica delle procedure di voto del Comitato, prevedendosi che nelle materie di competenza comunitaria, le Comunità europee esercitino il diritto di voto esprimendo un numero di voti pari al numero dei Paesi membri dell'Unione che non si sono avvalsi della c.d. clausola dell'*opting out* prevista dal Trattato di Amsterdam, liberi questi ultimi (Regno Unito, Irlanda e Danimarca) di accettare caso per caso il coordinamento comunitario.

Sono state modificate di conseguenza le disposizioni del regolamento interno per tutelare gli Stati-parte che non sono membri dell'Unione qualora, vertendosi in materie attribuite alle competenze comunitarie, gli Stati dell'Ue votino attraverso la Commissione europea.

A seguito del mandato conferito dal T-PD a un gruppo ristretto di lavoro per elaborare proposte per migliorare l'applicazione della Convenzione, con specifico riferimento all'opportunità di introdurre disposizioni volte a favorire la creazione di autorità di controllo indipendenti, a disciplinare i flussi verso Paesi terzi e a estendere le disposizioni della Convenzione agli archivi non automatizzati, sono state prospettate diverse soluzioni sulle quali peraltro non è stato ancora definito un consenso.

In particolare il gruppo ha preparato un progetto di Protocollo addizionale alla Convenzione, facoltativo per i Paesi che intendano accedere alla Convenzione stessa, per gli aspetti relativi alle autorità di controllo e ai flussi transfrontalieri; ha proposto altresì una Raccomandazione per gli aspetti relativi all'estensione del campo di applicazione della Convenzione.

Entrambi i temi formano oggetto di previa concertazione comunitaria in seno al gruppo problemi economici-protezione dati dell'Ue: i Paesi dell'Unione si presentano quindi, ove il diritto comunitario non lasci discrezionalità ai singoli Stati, in forma unitaria ed esprimono le loro posizioni attraverso la Commissione.

Il Gruppo di progetto sulla protezione dei dati - CJ-PD, ha approvato le *Linee-guida per la protezione della privacy in Internet* e ha predisposto il progetto della Raccomandazione poi approvata con il n. N.R (99)5 già citata.

Il CJ-PD ha inoltre proseguito la discussione per giungere all'adozione di una Raccomandazione sulla protezione dei dati nel settore delle assicurazioni. Anche in questo caso la materia è oggetto di previa concertazione comunitaria presso il gruppo problemi economici-protezione dei dati del Consiglio.

Il Gruppo di lavoro sulle nuove tecnologie - GT-15, gruppo ristretto costituito all'interno del CJ-PD, si è infine occupato del progetto di Raccomandazione sulla protezione dei dati raccolti e trattati a fini di sorveglianza.

4.5 OCSE

Particolarmente importanti i lavori svolti in seno al comitato ICCP per definire e predisporre il testo della dichiarazione sulla tutela della riservatezza da adottarsi da parte dei ministri partecipanti alla Conferenza mondiale di Ottawa sul commercio elettronico.

Nell'occasione sono state riviste, adeguandole, le linee-guida adottate dall'Organizzazione nel 1981.

La Conferenza, al di là degli specifici risultati raggiunti con l'approvazione di tre documenti e la definizione di un piano d'azione, ha avuto un ruolo molto importante, costituendo un momento di incontro e confronto tra Paesi portatori in materia di filosofie del tutto divergenti.

Al Garante è stato chiesto di presiedere, nella persona del suo Presidente, la delegazione italiana.

L'apporto fornito dai componenti del Garante ha permesso di tener conto di alcune esigenze in materia di tutela dei diritti fondamentali della persona, e di sviluppare riflessioni basate anche sui risultati delle Linee-guida approvate dall'OCSE nel 1980.

La dichiarazione finale della Conferenza sottolinea la necessità che le tematiche del commercio elettronico siano affrontate in modo da tenere conto dei diversi ruoli e dei diversi soggetti che vi partecipano (tra cui rappresentanti governativi, Autorità indipendenti, imprese private, associazioni rappresentative di utenti,) attraverso un approccio globale utile a favorire il più possibile la collaborazione e l'incontro delle volontà e degli interessi dei soggetti coinvolti.

4.6 COLLABORAZIONE CON AUTORITÀ DI GARANZIA DI ALTRI PAESI

Oltre agli obblighi di collaborazione con le altre Autorità di controllo nascenti dalla Convenzione n. 108 e da altri atti internazionali e comunitari, come ad esempio l'accordo di Schengen e la convenzione Europol, il Garante ha continuato a mante-

nere nel corso dell'anno stretti contatti con tali istituzioni per favorire lo scambio di esperienze e opinioni, anche al fine di raggiungere, ove possibile, interpretazioni convergenti od omogenee.

Il Garante ha inoltre partecipato con assiduità a numerose conferenze europee e mondiali che, per la loro rilevanza e la natura dei temi trattati, hanno rappresentato un importante foro di discussione e hanno consentito un puntuale aggiornamento.

Sono state, in particolare seguite le Conferenze internazionali ed europee delle Autorità garanti, che sono organizzate con criteri di periodicità, preferibilmente nella primavera e autunno di ogni anno.

Nel corso del 1998 la conferenza europea si è tenuta a Dublino il 23 e 24 aprile 1998 e quella mondiale a Santiago de Compostela il 16-18 settembre 1998.

Da segnalare la particolare attenzione rivolta dalle Autorità europee agli strumenti elaborati o in corso di elaborazione nell'ambito della cooperazione affari interni e giustizia che prevedono l'istituzione di sistemi di scambi di dati personali e la necessità di armonizzare le varie disposizioni, sostanziali e procedurali. A tal fine a Dublino, le Autorità hanno adottato una risoluzione con la quale auspicano l'adozione di iniziative in materia.(v. cap. 4.3).

In occasione dello svolgimento della conferenza internazionale, tenutasi a Santiago de Compostela, le Autorità garanti europee hanno approvato due dichiarazioni relative l'una allo sviluppo di Internet e alla tutela della privacy e, l'altra, al progetto del Governo islandese volto a istituire una base di dati di natura sanitaria, ivi compresi i dati genetici (nel quale si esprimono profonde preoccupazioni al riguardo e si riafferma l'esigenza di rispettare i principi contenuti nella convenzione n. 108 e nella Raccomandazione (97) 5 del Consiglio d'Europa, nonché quelli della direttiva 95/46/CE).

L'incontro periodico dell'Autorità comune di controllo Schengen si è svolto a Lisbona il 29 e 30 giugno 1998.

4.7 PARTECIPAZIONE A CONVEGNI E INCONTRI INTERNAZIONALI

Tra le varie iniziative di livello internazionale nelle quali il Garante ha avuto modo di fornire un proprio contributo alla discussione, oltre alla partecipazione alle Conferenze periodiche delle autorità di cui si è già fatto cenno, si possono citare le seguenti:

- The Eight Annual Conference on Computers, Freedom and Privacy, Austin Tx, 18-20 febbraio 1998;
- Convegno sulla firma digitale e cifratura Copenhagen, 23-24 aprile 1998;
- Riunione OCSE in materia di *privacy* e commercio elettronico, Parigi, 18 e 19 maggio 1998;
- *EPIC 98 - Cryptography and privacy Conference*, Washington, 8 giugno 1998;
- *The Protection of Personal data and the Media*, Seminario organizzato dall'Academy of European Law ERA di Trier/Treviri;
- *OECD Ministerial Conference «A borderless world: realising the potential of global electronic commerce»*, Ottawa, Canada, 7-9 ottobre 1998;
- *24th Meeting of the International Working Group on data protection in telecommunication* Berlino, 9 e 10 novembre 1998 (*Internet*; crittografia; legislazione in materia di telecomunicazioni).

5. ALLEGATI

5.1 LEGGE N. 675 DEL 31 DICEMBRE 1996

«Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»

Testo aggiornato in base ai seguenti decreti legislativi:

- n. **51** del **26 febbraio 1999**
- n. **389** del **6 novembre 1998**
- n. **171** del **13 maggio 1998**
- n. **135** dell'**8 maggio 1998**
- n. **255** del **28 luglio 1997**
- n. **123** del **9 maggio 1997**

CAPO I

PRINCIPI GENERALI

Art. 1.

(Finalità e definizioni)

1. La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.

2. Ai fini della presente legge si intende:

a) per «banca di dati», qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento;

b) per «trattamento», qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati;

c) per «dato personale», qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

d) per «titolare», la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;

e) per «responsabile», la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

f) per «interessato», la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

g) per «comunicazione», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) per «diffusione», il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) per «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

l) per «blocco», la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

m) per «Garante», l'autorità istituita ai sensi dell'articolo 30.

Art. 2.

(Ambito di applicazione)

1. La presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato.

Art. 3.

(Trattamento di dati per fini esclusivamente personali)

1. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della presente legge, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione.

2. Al trattamento di cui al comma 1 si applicano in ogni caso le disposizioni in tema di sicurezza dei dati di cui all'articolo 15, nonché le disposizioni di cui agli articoli 18 e 36.

Art. 4.

(Particolari trattamenti in ambito pubblico)

1. La presente legge non si applica al trattamento di dati personali effettuato:

a) dal Centro elaborazione dati di cui all'articolo 8 della legge 1 aprile 1981, n. 121, come modificato dall'articolo 43, comma 1, della presente legge, ovvero sui dati destinati a confluire in base alla legge, nonché in virtù dell'accordo di adesione alla Convenzione di applicazione dell'Accordo di Schengen, reso esecutivo con legge 30 settembre 1993, n. 388;

b) dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge;

c) nell'ambito del servizio del casellario giudiziale di cui al titolo IV del libro decimo del codice di procedura penale e al regio decreto 18 giugno 1931, n. 778, e successive modificazioni, o, in base alla legge, nell'ambito del servizio dei carichi pendenti nella materia penale;

d) in attuazione dell'articolo 371-bis, comma 3, del codice di procedura penale o, per ragioni di giustizia, nell'ambito di uffici giudiziari, del Consiglio superiore della magistratura e del Ministero di grazia e giustizia;

e) da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento.

2. Ai trattamenti di cui al comma 1 si applicano in ogni caso le disposizioni di cui agli articoli 9, 15, 17, 18, 31, 32, commi 6 e 7 e 36, nonché, fatta eccezione per i trattamenti di cui alla lettera b) del comma 1, le disposizioni di cui agli articoli 7 e 34.

Art. 5.

(Trattamento di dati svolto senza l'ausilio di mezzi elettronici)

1. Il trattamento di dati personali svolto senza l'ausilio di mezzi elettronici o comunque automatizzati è soggetto alla medesima disciplina prevista per il trattamento effettuato con l'ausilio di tali mezzi.

Art. 6.

(Trattamento di dati detenuti all'estero)

1. Il trattamento nel territorio dello Stato di dati personali detenuti all'estero è soggetto alle disposizioni della presente legge.

2. Se il trattamento di cui al comma 1 consiste in un trasferimento di dati personali fuori dal territorio nazionale si applicano in ogni caso le disposizioni dell'articolo 28.

CAPO II

OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Art. 7.

(Notificazione)

1. Il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne notificazione al Garante.

2. La notificazione è effettuata preventivamente ed una sola volta, a mezzo di lettera raccomandata ovvero con altro mezzo idoneo a certificarne la ricezione, a prescindere dal numero delle operazioni da svolgere, nonché dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo se muta taluno degli elementi indicati nel comma 4 e deve precedere l'effettuazione della variazione.

3. La notificazione è sottoscritta dal notificante e dal responsabile del trattamento.

4. La notificazione contiene:

- a) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare;
- b) le finalità e modalità del trattamento;
- c) la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
- d) l'ambito di comunicazione e di diffusione dei dati;
- e) i trasferimenti di dati previsti verso Paesi non appartenenti all'Unione europea o, qualora riguardino taluno dei dati di cui agli articoli 22 e 24, fuori del territorio nazionale;
- f) una descrizione generale che permetta di valutare l'adeguatezza delle misure tecniche ed organizzative adottate per la sicurezza dei dati;
- g) l'indicazione della banca di dati o delle banche di dati cui si riferisce il trattamento, nonché l'eventuale connessione con altri trattamenti o banche di dati, anche fuori del territorio nazionale;
- h) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del responsabile; in mancanza di tale indicazione si considera responsabile il notificante;
- i) la qualità e la legittimazione del notificante.

5. I soggetti tenuti ad iscriversi o che devono essere annotati nel registro delle imprese di cui all'articolo 2188 del codice civile, nonché coloro che devono fornire le informazioni di cui all'articolo 8, comma 8, lettera d), della legge 29 dicembre 1993, n. 580, alle camere di commercio, industria, artigianato e agricoltura, possono effettuare la notificazione per il tramite di queste ultime, secondo le modalità stabilite con il regolamento di cui all'articolo 33, comma 3. I piccoli imprenditori e gli artigiani possono effettuare la notificazione anche per il tramite delle rispettive rappresentanze di categoria; gli iscritti agli albi professionali anche per il tramite dei rispettivi ordini professionali. Resta in ogni caso ferma la disposizione di cui al comma 3.

5-bis ¹⁾. La notificazione in forma semplificata può non contenere taluno degli elementi di cui al comma 4, lettere b), c), e) e g), individuati dal Garante ai sensi del regolamento di cui all'articolo 33, comma 3, quando il trattamento è effettuato:

a) da soggetti pubblici, esclusi gli enti pubblici economici, sulla base di espressa disposizione di legge ai sensi degli articoli 22, comma 3 e 24, ovvero del provvedimento di cui al medesimo articolo 24;

¹⁾ Commi aggiunti dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

b) nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità, ovvero dai soggetti indicati nel comma 4-bis dell'articolo 25, nel rispetto del codice di deontologia di cui al medesimo articolo;

c) temporaneamente senza l'ausilio di mezzi elettronici o comunque automatizzati, ai soli fini e con le modalità strettamente collegate all'organizzazione interna dell'attività esercitata dal titolare, relativamente a dati non registrati in una banca di dati e diversi da quelli di cui agli articoli 22 e 24.

5-ter ¹⁾. Fuori dei casi di cui all'articolo 4, il trattamento non è soggetto a notificazione quando:

a) è necessario per l'assolvimento di un compito previsto dalla legge, da un regolamento o dalla normativa comunitaria, relativamente a dati diversi da quelli indicati negli articoli 22 e 24;

b) riguarda dati contenuti o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità di cui all'articolo 20, comma 1, lettera b);

c) è effettuato per esclusive finalità di gestione del protocollo, relativamente ai dati necessari per la classificazione della corrispondenza inviata per fini diversi da quelli di cui all'articolo 13, comma 1, lettera e), con particolare riferimento alle generalità e ai recapiti degli interessati, alla loro qualifica e all'organizzazione di appartenenza;

d) riguarda rubriche telefoniche o analoghe non destinate alla diffusione, utilizzate unicamente per ragioni d'ufficio e di lavoro e comunque per fini diversi da quelli di cui all'articolo 13, comma 1, lettera e);

e) è finalizzato unicamente all'adempimento di specifici obblighi contabili, retributivi, previdenziali, assistenziali e fiscali, ed è effettuato con riferimento alle sole categorie di dati, di interessati e di destinatari della comunicazione e diffusione strettamente collegate a tale adempimento, conservando i dati non oltre il periodo necessario all'adempimento medesimo;

f) è effettuato, salvo quanto previsto dal comma 5-bis, lettera b), da liberi professionisti iscritti in albi o elenchi professionali, per le sole finalità strettamente collegate all'adempimento di specifiche prestazioni e fermo restando il segreto professionale;

g) è effettuato dai piccoli imprenditori di cui all'articolo 2083 del codice civile per le sole finalità strettamente collegate allo svolgimento dell'attività professionale esercitata, e limitatamente alle categorie di dati, di interessati, di destinatari della comunicazione e diffusione e al periodo di conservazione dei dati necessari per il perseguimento delle finalità medesime;

h) è finalizzato alla tenuta di albi o elenchi professionali in conformità alle leggi e ai regolamenti;

i) è effettuato per esclusive finalità dell'ordinaria gestione di biblioteche, musei e mostre, in conformità alle leggi e ai regolamenti, ovvero per la organizzazione di iniziative culturali o sportive o per la formazione di cataloghi e bibliografie;

¹⁾ Commi aggiunti dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

l) è effettuato da associazioni, fondazioni, comitati anche a carattere politico, filosofico, religioso o sindacale, ovvero da loro organismi rappresentativi, istituiti per scopi non di lucro e per il perseguimento di finalità lecite, relativamente a dati inerenti agli associati e ai soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, la fondazione, il comitato o l'organismo, fermi restando gli obblighi di informativa degli interessati e di acquisizione del consenso, ove necessario;

m) è effettuato dalle organizzazioni di volontariato di cui alla legge 11 agosto 1991, n. 266, nei limiti di cui alla lettera l) e nel rispetto delle autorizzazioni e delle prescrizioni di legge di cui agli articoli 22 e 23;

n) è effettuato temporaneamente ed è finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero, nel rispetto del codice di deontologia di cui all'articolo 25;

o) è effettuato, anche con mezzi elettronici o comunque automatizzati, per la redazione di periodici o pubblicazioni aventi finalità di informazione giuridica, relativamente a dati desunti da provvedimenti dell'autorità giudiziaria o di altre autorità;

p) è effettuato temporaneamente per esclusive finalità di raccolta di adesioni a proposte di legge d'iniziativa popolare, a richieste di referendum, a petizioni o ad appelli;

q) è finalizzato unicamente all'amministrazione dei condomini di cui all'articolo 1117 e seguenti del codice civile, limitatamente alle categorie di dati, di interessati e di destinatari della comunicazione necessarie per l'amministrazione dei beni comuni, conservando i dati non oltre il periodo necessario per la tutela dei corrispondenti diritti.

5-quater¹⁾. Il titolare si può avvalere della notificazione semplificata o dell'esonero di cui ai commi 5-bis e 5-ter, sempre che il trattamento riguardi unicamente le finalità, le categorie di dati, di interessati e di destinatari della comunicazione e diffusione, individuate, unitamente al periodo di conservazione dei dati, dai medesimi commi 5-bis e 5-ter, nonché:

a) nei casi di cui ai commi 5-bis, lettera a) e 5-ter, lettere a) e m), dalle disposizioni di legge o di regolamento o dalla normativa comunitaria ivi indicate;

b) nel caso di cui al comma 5-bis, lettera b), dal codice di deontologia ivi indicato;

c) nei casi residui, dal Garante con le autorizzazioni rilasciate con le modalità previste dall'articolo 41, comma 7, ovvero, per i dati diversi da quelli di cui agli articoli 22 e 24, con provvedimenti analoghi.

5-quinquies¹⁾. Il titolare che si avvale dell'esonero di cui al comma 5-ter deve fornire gli elementi di cui al comma 4 a chiunque ne faccia richiesta.

Art. 8. (Responsabile)

1. Il responsabile, se designato, deve essere nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

¹⁾ Commi aggiunti dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

2. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.

5. Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.

CAPO III

TRATTAMENTO DEI DATI PERSONALI

Sezione I

RACCOLTA E REQUISITI DEI DATI

Art. 9.

(Modalità di raccolta e requisiti dei dati personali)

1. I dati personali oggetto di trattamento devono essere:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Art. 10.

(Informazioni rese al momento della raccolta)

1. ²⁾ L'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati *oralmente o per iscritto* circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'articolo 13;
- f) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile.

²⁾ Comma così modificato dall'art. 1, d.lg. 9 maggio 1997, n. 123.

2. L'informativa di cui al comma 1 può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare l'espletamento di funzioni pubbliche ispettive o di controllo, svolte per il perseguimento delle finalità di cui agli articoli 4, comma 1, lettera e), e 14, comma 1, lettera d).

3. Quando i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1 è data al medesimo interessato all'atto della registrazione dei dati o, qualora sia prevista la loro comunicazione, non oltre la prima comunicazione.

4. La disposizione di cui al comma 3 non si applica quando l'informativa all'interessato comporta un impiego di mezzi che il Garante dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si rivela, a giudizio del Garante, impossibile, ovvero nel caso in cui i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. La medesima disposizione non si applica, altresì, quando i dati sono trattati ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Sezione II

DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Art. 11.

(Consenso)

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 10.

Art. 12.

(Casi di esclusione del consenso)

1. Il consenso non è richiesto quando il trattamento:

a) riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'acquisizione di informative precontrattuali attivate su richiesta di quest'ultimo, ovvero per l'adempimento di un obbligo legale;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

d) è finalizzato unicamente a scopi di ricerca scientifica o di statistica e si tratta di dati anonimi;

e) ³⁾ è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. *In tale caso, si applica il codice di deontologia di cui all'articolo 25;*

f) riguarda dati relativi allo svolgimento di attività economiche raccolti anche ai fini indicati nell'articolo 13, comma 1, lettera e), nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;

h) è necessario ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Art. 13.

(Diritti dell'interessato)

1. In relazione al trattamento di dati personali l'interessato ha diritto:

a) di conoscere, mediante accesso gratuito al registro di cui all'articolo 31, comma 1, lettera a), l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato su quanto indicato all'articolo 7, comma 4, lettere a), b) e h);

c) di ottenere, a cura del titolare o del responsabile, senza ritardo:

1) la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;

2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

3) l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;

4) l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

d) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

e) di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di co-

³⁾ Lettera così modificata dall'art. 12, comma 1, d.lg. 13 maggio 1998, n. 171.

municazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

2. Per ciascuna richiesta di cui al comma 1, lettera c), numero 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati, secondo le modalità ed entro i limiti stabiliti dal regolamento di cui all'articolo 33, comma 3.

3. I diritti di cui al comma 1 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia interesse.

4. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

5. Restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

Art. 14.

(Limiti all'esercizio dei diritti)

1. I diritti di cui all'articolo 13, comma 1, lettere c) e d), non possono essere esercitati nei confronti dei trattamenti di dati personali raccolti:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti la politica monetaria e valutaria, il sistema dei pagamenti, il controllo degli intermediari e dei mercati creditizi e finanziari nonché la tutela della loro stabilità;

e) ai sensi dell'articolo 12, comma 1, lettera h), limitatamente al periodo durante il quale potrebbe derivarne pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto di cui alla medesima lettera h).

2. Nei casi di cui al comma 1 il Garante, anche su segnalazione dell'interessato ai sensi dell'articolo 31, comma 1, lettera d), esegue i necessari accertamenti nei modi di cui all'articolo 32, commi 6 e 7, e indica le necessarie modificazioni ed integrazioni, verificandone l'attuazione.

Sezione III

SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITÀ DEI DATI E RISARCIMENTO DEL DANNO

Art. 15.

(Sicurezza dei dati)

1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da

ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

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

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

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

Art. 16.

(Cessazione del trattamento dei dati)

1. In caso di cessazione, per qualsiasi causa, del trattamento dei dati, il titolare deve notificare preventivamente al Garante la loro destinazione.

2. I dati possono essere:

- a) distrutti;
- b) ceduti ad altro titolare, purché destinati ad un trattamento per finalità analoghe agli scopi per i quali i dati sono raccolti;
- c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione.

3. La cessione dei dati in violazione di quanto previsto dalla lettera b) del comma 2 o di altre disposizioni di legge in materia di trattamento dei dati personali è nulla ed è punita ai sensi dell'articolo 39, comma 1.

Art. 17.

(Limiti all'utilizzabilità di dati personali)

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

2. L'interessato può opporsi ad ogni altro tipo di decisione adottata sulla base del trattamento di cui al comma 1 del presente articolo, ai sensi dell'articolo 13, comma 1, lettera d), salvo che la decisione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dalla legge.

Art. 18.***(Danni cagionati per effetto del trattamento di dati personali)***

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

Sezione IV**COMUNICAZIONE E DIFFUSIONE DEI DATI****Art. 19.*****(Incaricati del trattamento)***

1. Non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità.

Art. 20.***(Requisiti per la comunicazione e la diffusione dei dati)***

1. La comunicazione e la diffusione dei dati personali da parte di privati e di enti pubblici economici sono ammesse:

- a) con il consenso espresso dell'interessato;
- b) se i dati provengono da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi e i regolamenti stabiliscono per la loro conoscibilità e pubblicità;
- c) in adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- d) ⁴⁾ nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. *Restano fermi i limiti del diritto di cronaca posti a tutela della riservatezza ed in particolare dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Si applica inoltre il codice di deontologia di cui all'articolo 25;*
- e) se i dati sono relativi allo svolgimento di attività economiche, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- f) qualora siano necessarie per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;
- g) limitatamente alla comunicazione, qualora questa sia necessaria ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere un diritto in sede giudiziaria, nel rispetto della normativa di cui alla lettera e) del presente comma, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

⁴⁾ Lettera così modificata dall'art. 12, comma 2, d.lg. 13 maggio 1998, n. 171.

h) limitatamente alla comunicazione, quando questa sia effettuata nell'ambito dei gruppi bancari di cui all'articolo 60 del testo unico delle leggi in materia bancaria e creditizia approvato con decreto legislativo 1 settembre 1993, n. 385, nonché tra società controllate e società collegate ai sensi dell'articolo 2359 del codice civile, i cui trattamenti con finalità correlate sono stati notificati ai sensi dell'articolo 7, comma 2, per il perseguimento delle medesime finalità per le quali i dati sono stati raccolti.

2. Alla comunicazione e alla diffusione dei dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, si applicano le disposizioni dell'articolo 27.

Art. 21.

(Divieto di comunicazione e diffusione)

1. Sono vietate la comunicazione e la diffusione di dati personali per finalità diverse da quelle indicate nella notificazione di cui all'articolo 7.

2. Sono altresì vietate la comunicazione e la diffusione di dati personali dei quali sia stata ordinata la cancellazione, ovvero quando sia decorso il periodo di tempo indicato nell'articolo 9, comma 1, lettera e).

3. Il Garante può vietare la diffusione di taluno dei dati relativi a singoli soggetti, od a categorie di soggetti, quando la diffusione si pone in contrasto con rilevanti interessi della collettività. Contro il divieto può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

4. La comunicazione e la diffusione dei dati sono comunque permesse:

a) qualora siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi;

b) quando siano richieste dai soggetti di cui all'articolo 4, comma 1, lettere b), d) ed e), per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia.

CAPO IV

TRATTAMENTO DI DATI PARTICOLARI

Art. 22.

(Dati sensibili)

1. I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro trenta giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il trattamento dei dati indicati al comma 1 da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

4. I dati personali idonei a rivelare lo stato di salute e la vita sessuale possono essere oggetto di trattamento previa autorizzazione del Garante, qualora il trattamento sia necessario ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Il Garante prescrive le misure e gli accorgimenti di cui al comma 2 e promuove la sottoscrizione di un apposito codice di deontologia e di buona condotta secondo le modalità di cui all'articolo 31, comma 1, lettera h). Resta fermo quanto previsto dall'articolo 43, comma 2.

Art. 23.

(Dati inerenti alla salute)

1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possono, anche senza l'autorizzazione del Garante, trattare i dati personali idonei a rivelare lo stato di salute, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato. Se le medesime finalità riguardano un terzo o la collettività, in mancanza del consenso dell'interessato, il trattamento può avvenire previa autorizzazione del Garante.

2. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo per il tramite di un medico designato dall'interessato o dal titolare.

3. L'autorizzazione di cui al comma 1 è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità. È vietata la comunicazione dei dati ottenuti oltre i limiti fissati con l'autorizzazione.

4. La diffusione dei dati idonei a rivelare lo stato di salute è vietata, salvo nel caso in cui sia necessaria per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

Art. 24.

(Dati relativi ai provvedimenti di cui all'articolo 686 del codice di procedura penale)

1. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, è ammesso soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni autorizzate.

Art. 25.

(Trattamento di dati particolari nell'esercizio della professione di giornalista)

1.⁵⁾ *Le disposizioni relative al consenso dell'interessato e all'autorizzazione del Garante, nonché il limite previsto dall'articolo 24, non si applicano quando il trattamento dei dati di cui agli articoli 22 e 24 è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. Il giornalista rispetta i limiti del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, ferma restando la possibilità di trattare i dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico.*

2.⁶⁾ Il Garante promuove, nei modi di cui all'articolo 31, comma 1, lettera h), l'adozione, da parte del Consiglio nazionale dell'ordine dei giornalisti, di un apposito codice di deontologia relativo al trattamento dei dati di cui al comma 1 del presente articolo effettuato nell'esercizio della professione di giornalista, che preveda misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, *in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale*. Nella fase di formazione del codice, ovvero successivamente, il Garante *in cooperazione con il Consiglio*, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire. *Il Codice è pubblicato sulla Gazzetta Ufficiale a cura del Garante, e diviene efficace quindici giorni dopo la sua pubblicazione.*

3. Ove entro sei mesi dalla proposta del Garante il codice di deontologia di cui al comma 2 non sia stato adottato dal Consiglio nazionale dell'Ordine dei giornalisti, esso è adottato in via sostitutiva dal Garante ed è efficace sino alla adozione di un diverso codice secondo la procedura di cui al comma 2. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 31, comma 1, lettera l).

4.⁷⁾ Nel codice di cui ai commi 2 e 3 sono inserite, altresì, prescrizioni concernenti i dati personali diversi da quelli indicati negli articoli 22 e 24. *Il codice può prevedere forme semplificate per le informative di cui all'articolo 10.*

4-bis.⁸⁾ *Le disposizioni della presente legge che attengono all'esercizio della professione di giornalista si applicano anche ai trattamenti effettuati dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli articoli 26*

⁵⁾ Comma così sostituito dall'art. 12, comma 3, d.lg. 13 maggio 1998, n. 171.

⁶⁾ Comma così modificato dall'art. 12, comma 4, d.lg. 13 maggio 1998, n. 171.

⁷⁾ Comma così modificato dall'art. 2, comma 1, d.lg. 9 maggio 1997, n. 123.

⁸⁾ Comma aggiunto dall'art. 2, comma 2, d.lg. 9 maggio 1997, n. 123.

e 33 della legge 3 febbraio 1963, n. 69, nonché ai trattamenti temporanei finalizzati esclusivamente alla pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero.

Art. 26.

(Dati concernenti persone giuridiche)

1. Il trattamento nonché la cessazione del trattamento di dati concernenti persone giuridiche, enti o associazioni non sono soggetti a notificazione.

2. Ai dati riguardanti persone giuridiche, enti o associazioni non si applicano le disposizioni dell'articolo 28.

CAPO V

TRATTAMENTI SOGGETTI A REGIME SPECIALE

Art. 27.

(Trattamento da parte di soggetti pubblici)

1. Salvo quanto previsto al comma 2, il trattamento di dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti.

2. La comunicazione e la diffusione a soggetti pubblici, esclusi gli enti pubblici economici, dei dati trattati sono ammesse quando siano previste da norme di legge o di regolamento, o risultino comunque necessarie per lo svolgimento delle funzioni istituzionali. In tale ultimo caso deve esserne data previa comunicazione nei modi di cui all'articolo 7, commi 2 e 3 al Garante che vieta, con provvedimento motivato, la comunicazione o la diffusione se risultano violate le disposizioni della presente legge.

3. La comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o a enti pubblici economici sono ammesse solo se previste da norme di legge o di regolamento.

4. I criteri di organizzazione delle amministrazioni pubbliche di cui all'articolo 5 del decreto legislativo 3 febbraio 1993, n. 29, sono attuati nel pieno rispetto delle disposizioni della presente legge.

Art. 28.

(Trasferimento di dati personali all'estero)

1. Il trasferimento anche temporaneo fuori del territorio nazionale, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento deve essere previamente notificato al Garante, qualora sia diretto verso un Paese non appartenente all'Unione europea o riguardi taluno dei dati di cui agli articoli 22 e 24.

2. Il trasferimento può avvenire soltanto dopo quindici giorni dalla data della notificazione; il termine è di venti giorni qualora il trasferimento riguardi taluno dei dati di cui agli articoli 22 e 24.

3. Il trasferimento è vietato qualora l'ordinamento dello Stato di destinazione o di transito dei dati non assicuri un livello di tutela delle persone adeguato ovvero, se si tratta dei dati di cui agli articoli 22 e 24, di grado pari a quello assicurato dall'ordinamento italiano. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

4. Il trasferimento è comunque consentito qualora:

a) l'interessato abbia manifestato il proprio consenso espresso ovvero, se il trasferimento riguarda taluno dei dati di cui agli articoli 22 e 24, in forma scritta;

b) sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'acquisizione di informative precontrattuali attivate su richiesta di quest'ultimo, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) sia necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento, ovvero specificato ai sensi degli articoli 22, comma 3 e 24, se il trasferimento riguarda taluno dei dati ivi previsti;

d) sia necessario ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

e) sia necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;

f) sia effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto.

5. Contro il divieto di cui al comma 3 del presente articolo può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

6. Le disposizioni del presente articolo non si applicano al trasferimento di dati personali effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità.

7. La notificazione di cui al comma 1 del presente articolo è effettuata ai sensi dell'articolo 7 ed è annotata in apposita sezione del registro previsto dall'articolo 31, comma 1, lettera a). La notificazione può essere effettuata con un unico atto unitamente a quella prevista dall'articolo 7.

CAPO VI
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 29.
(Tutela)

1. I diritti di cui all'articolo 13, comma 1, possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante. Il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria.

2. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che siano decorsi cinque giorni dalla richiesta avanzata sul medesimo oggetto al responsabile. La presentazione del ricorso rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. Il Garante può disporre, anche d'ufficio, l'espletamento di perizie.

4. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare e al responsabile, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. Il provvedimento è comunicato senza ritardo alle parti interessate, a cura dell'ufficio del Garante. La mancata pronuncia sul ricorso, decorsi venti giorni dalla data di presentazione, equivale a rigetto.

5. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento cessa di avere ogni effetto se, entro i successivi venti giorni, non è adottata la decisione di cui al comma 4 ed è impugnabile unitamente a tale decisione.

6. Avverso il provvedimento espresso o il rigetto tacito di cui al comma 4, il titolare o l'interessato possono proporre opposizione al tribunale del luogo ove risiede il titolare, entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. L'opposizione non sospende l'esecuzione del provvedimento.

7. Il tribunale provvede nei modi di cui agli articoli 737 e seguenti del codice di procedura civile, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), e può sospendere, a richiesta, l'esecuzione del provvedimento. Avverso il decreto del tribunale è ammesso unicamente il ricorso per cassazione.

8. Tutte le controversie, ivi comprese quelle inerenti il rilascio dell'autorizzazione di cui all'articolo 22, comma 1, o che riguardano, comunque, l'applicazione della presente legge, sono di competenza dell'autorità giudiziaria ordinaria.

9. Il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 9.

CAPO VII
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI ⁹⁾

Art. 30.
(Istituzione del Garante)

1. ¹⁰⁾ È istituito il *Garante per la protezione dei dati personali*.
2. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.
3. Il Garante è organo collegiale costituito da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. Essi eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza delle materie del diritto o dell'informatica, *garantendo la presenza di entrambe le qualificazioni*.
4. Il presidente e i membri durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i membri non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.
5. All'atto dell'accettazione della nomina il presidente e i membri sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.
6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai membri compete un'indennità di funzione non eccedente, nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate, con il regolamento di cui all'articolo 33, comma 3, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

Art. 31.
(Compiti del Garante)

1. Il Garante ha il compito di:
 - a) istituire e tenere un registro generale dei trattamenti sulla base delle notificazioni ricevute;
 - b) controllare se i trattamenti sono effettuati nel rispetto delle norme di legge e di regolamento e in conformità alla notificazione;
 - c) segnalare ai relativi titolari o responsabili le modificazioni opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;

⁹⁾ Denominazione così modificata dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.

¹⁰⁾ Comma così modificato dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.

d) ricevere le segnalazioni ed i reclami degli interessati o delle associazioni che li rappresentano, relativi ad inosservanze di legge o di regolamento, e provvedere sui ricorsi presentati ai sensi dell'articolo 29;

e) adottare i provvedimenti previsti dalla legge o dai regolamenti;

f) vigilare sui casi di cessazione, per qualsiasi causa, di un trattamento;

g) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle sue funzioni;

h) promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

i) curare la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità, nonché delle misure di sicurezza dei dati di cui all'articolo 15;

l) vietare, in tutto o in parte, il trattamento dei dati o disporre il blocco quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

m) segnalare al Governo l'opportunità di provvedimenti normativi richiesti dall'evoluzione del settore;

n) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione della presente legge, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce;

o) curare l'attività di assistenza indicata nel capitolo IV della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della Convenzione medesima;

p) esercitare il controllo sui trattamenti di cui all'articolo 4 e verificare, anche su richiesta dell'interessato, se rispondono ai requisiti stabiliti dalla legge o dai regolamenti.

2. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla presente legge.

3. Il registro di cui al comma 1, lettera a), del presente articolo, è tenuto nei modi di cui all'articolo 33, comma 5. Entro il termine di un anno dalla data della sua istituzione, il Garante promuove opportune intese con le province ed eventualmente con altre pubbliche amministrazioni al fine di assicurare la consultazione del registro mediante almeno un terminale dislocato su base provinciale, preferibilmente nell'ambito dell'ufficio per le relazioni con il pubblico di cui all'articolo 12 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni.

4. Contro il divieto di cui al comma 1, lettera l), del presente articolo, può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

5. Il Garante e l'Autorità per l'informatica nella pubblica amministrazione cooperano tra loro nello svolgimento dei rispettivi compiti; a tal fine, invitano il presidente o un suo delegato membro dell'altro organo a partecipare alle

riunioni prendendo parte alla discussione di argomenti di comune interesse iscritti all'ordine del giorno; possono richiedere, altresì, la collaborazione di personale specializzato addetto all'altro organo.

6. Le disposizioni del comma 5 si applicano anche nei rapporti tra il Garante e le autorità di vigilanza competenti per il settore creditizio, per le attività assicurative e per la radiodiffusione e l'editoria.

Art. 32.

(Accertamenti e controlli)

1. Per l'espletamento dei propri compiti il Garante può richiedere al responsabile, al titolare, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

2. Il Garante, qualora ne ricorra la necessità ai fini del controllo del rispetto delle disposizioni in materia di trattamento dei dati personali, può disporre accessi alle banche di dati o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo, avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 2 sono disposti previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede senza ritardo sulla richiesta del Garante, con decreto motivato; le relative modalità di svolgimento sono individuate con il regolamento di cui all'articolo 33, comma 3.

4. I soggetti interessati agli accertamenti sono tenuti a farli eseguire.

5. Resta fermo quanto previsto dall'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

6. Per i trattamenti di cui agli articoli 4 e 14, comma 1, gli accertamenti sono effettuati per il tramite di un membro designato dal Garante. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, salvo che ricorrano i motivi di cui all'articolo 10, comma 4, della legge 1 aprile 1981, n. 121, come sostituito dall'articolo 42, comma 1, della presente legge, o motivi di difesa o di sicurezza dello Stato.

7. Gli accertamenti di cui al comma 6 non sono delegabili. Qualora risulti necessario in ragione della specificità della verifica, il membro designato può farsi assistere da personale specializzato che è tenuto al segreto ai sensi dell'articolo 33, comma 6. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai membri del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti al relativo ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 33, comma 3. Per gli accertamenti relativi agli organismi e ai dati di cui all'articolo 4, comma 1, lettera b), il membro designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

Art. 33.
(Ufficio del Garante)

1. Alle dipendenze del Garante è posto un ufficio composto, *in sede di prima applicazione della presente legge*,¹¹⁾ da dipendenti dello Stato e di altre amministrazioni pubbliche, collocati fuori ruolo nelle forme previste dai rispettivi ordinamenti, il cui servizio presso il medesimo ufficio è equiparato ad ogni effetto di legge a quello prestato nelle rispettive amministrazioni di provenienza. Il relativo contingente è determinato, in misura non superiore a quarantacinque unità, su proposta del Garante medesimo, con decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri del tesoro e per la funzione pubblica, entro novanta giorni dalla data di elezione del Garante. *Il segretario generale può essere scelto anche tra magistrati ordinari o amministrativi*^{12) 13)}.

1-bis¹⁴⁾ È istituito il ruolo organico del personale dipendente del Garante. Con proprio regolamento il Garante definisce: a) l'ordinamento delle carriere e le modalità del reclutamento secondo le procedure previste dall'articolo 36 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni; b) le modalità dell'inquadramento in ruolo del personale in servizio alla data dell'entrata in vigore del regolamento; c) il trattamento giuridico ed economico del personale secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e, per gli incarichi di funzioni dirigenziali, dall'articolo 19, comma 6, del citato decreto legislativo n. 29, come sostituito dall'articolo 13 del decreto legislativo 31 marzo 1998, n. 80, tenuto conto delle specifiche esigenze funzionali e organizzative. Il regolamento è pubblicato nella Gazzetta ufficiale. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni. Per il periodo intercorrente tra l'8 maggio 1997 e la data di entrata in vigore del regolamento, resta ferma l'indennità di cui all'articolo 41 del decreto del Presidente della Repubblica 10 luglio 1991, n. 231, corrisposta al personale in servizio. Dal 1 gennaio 1998 e fino alla data di entrata in vigore del medesimo regolamento, è inoltre corrisposta la differenza tra il nuovo trattamento e la retribuzione già in godimento maggiorata della predetta indennità di funzione.

1-ter¹⁴⁾. L'ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale

¹¹⁾ Parole inserite dall'art. 1, comma 1, d.lg. 26 febbraio 1999, n. 51.

¹²⁾ Parole aggiunte dall'art. 3, comma 2, d.lg. 9 maggio 1997, n. 123.

¹³⁾ L'art. 3, comma 3 del decreto legislativo 9 maggio 1997, n. 123, prevede che «Il personale richiesto dal Garante per la protezione dei dati personali nella fase di costituzione del relativo ufficio, nelle more del perfezionamento del comando, del fuori ruolo o dell'aspettativa, può essere utilizzato dal Garante a decorrere dalla data indicata nella richiesta, sempreché tale data sia di almeno dieci giorni successiva a quella della richiesta, vi sia l'assenso dell'interessato e l'amministrazione o l'ente di appartenenza non si opponga.»

¹⁴⁾ Commi aggiunti dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51.

di cui al presente comma è corrisposta una indennità pari alla eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al corrispondente personale di ruolo, e comunque non inferiore alla indennità di cui all'articolo 41 del citato decreto del Presidente della Repubblica n. 231.

1-quater.¹⁵⁾ Con proprio regolamento il Garante ripartisce l'organico, fissato nel limite di cento unità, tra il personale dei diversi livelli e quello delle qualifiche dirigenziali e disciplina l'organizzazione, il funzionamento dell'ufficio, la riscossione e la utilizzazione dei diritti di segreteria, ivi compresi quelli corrisposti dall'8 maggio 1997, e la gestione delle spese, anche in deroga alle norme sulla contabilità generale dello Stato. Il regolamento è pubblicato nella Gazzetta ufficiale.

1-quinquies.¹⁵⁾ In aggiunta al personale di ruolo, l'ufficio può assumere direttamente dipendenti con contratto a tempo determinato disciplinato dalle norme di diritto privato, in numero non superiore a venti unità, ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 4.

1-sexies.¹⁵⁾ All'ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e quelli concernenti le funzioni di gestione attribuite ai dirigenti.

2. Le spese di funzionamento dell'ufficio del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero del tesoro. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

3.¹⁶⁾ *In sede di prima applicazione della presente legge, le norme concernenti l'organizzazione ed il funzionamento dell'ufficio del Garante, nonché quelle dirette a disciplinare la riscossione dei diritti di segreteria e la gestione delle spese, anche in deroga alle disposizioni sulla contabilità generale dello Stato, sono adottate con regolamento emanato con decreto del Presidente della Repubblica, entro tre mesi dalla data di entrata in vigore della presente legge, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato, su proposta del Presidente del Consiglio dei ministri, di concerto con i Ministri del tesoro, di grazia e giustizia e dell'interno, e su parere conforme del Garante stesso. Nel medesimo regolamento sono determinate le indennità di cui all'articolo 30, comma 6, e altresì previste le norme concernenti il procedimento dinanzi al Garante di cui all'articolo 29, commi da 1 a 5, secondo modalità tali da assicurare, nella speditezza del procedimento medesimo, il pieno rispetto del contraddittorio tra le parti interessate, nonché le norme volte a precisare le modalità per l'esercizio dei diritti di cui all'art. 13, nonché della notificazione di cui all'articolo 7,*

¹⁵⁾ Commi aggiunti dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51.

¹⁶⁾ Comma così modificato dall'art. 2, comma 2, d.lg. 26 febbraio 1999, n. 51.

per via telematica o mediante supporto magnetico o lettera raccomandata con avviso di ricevimento o altro idoneo sistema. Il parere del Consiglio di Stato sullo schema di regolamento è reso entro trenta giorni dalla ricezione della richiesta; decorso tale termine il regolamento può comunque essere emanato.¹⁷⁾

3-bis.¹⁸⁾ *Con effetto dalla data di entrata in vigore del regolamento di cui al comma 1-quater, cessano di avere vigore le norme adottate ai sensi del comma 3, primo periodo.*

4.¹⁹⁾ Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedano, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

5. Per l'espletamento dei propri compiti, l'ufficio del Garante può avvalersi di sistemi automatizzati ad elaborazione informatica e di strumenti telematici propri ovvero, salvaguardando le garanzie previste dalla presente legge, appartenenti all'Autorità per l'informatica nella pubblica amministrazione o, in caso di indisponibilità, ad enti pubblici convenzionati.

6. Il personale addetto all'ufficio del Garante ed i consulenti sono tenuti al segreto su tutto ciò di cui siano venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a banche di dati e ad operazioni di trattamento.

6-bis.²⁰⁾ *Il personale dell'ufficio del Garante addetto agli accertamenti di cui all'articolo 32 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.*

CAPO VIII SANZIONI

Art. 34.

(Omessa o infedele notificazione)

1. Chiunque, essendovitenuto, non provvede alle notificazioni prescritte dagli articoli 7 e 28, ovvero indica in esse notizie incomplete o non rispondenti al vero, è punito con la reclusione da tre mesi a due anni. Se il fatto concerne la notificazione prevista dall'articolo 16, comma 1, la pena è della reclusione sino ad anno.

¹⁷⁾ L'art. 5, comma 3, del decreto legislativo 9 maggio 1997, n. 123, prevede che «Fino alla data di entrata in vigore del decreto di cui all'articolo 33, comma 3, della legge 31 dicembre 1996, n. 675, per la gestione delle spese dell'ufficio del Garante per la protezione dei dati personali si osservano, in quanto compatibili, le disposizioni contenute nel regolamento per la gestione delle spese occorrenti per il funzionamento dell'Autorità per l'informatica nella pubblica amministrazione, approvate con decreto del Presidente del Consiglio dei Ministri 6 ottobre 1994, n. 769, pubblicato nella Gazzetta Ufficiale n. 78 del 2 aprile 1995.»

¹⁸⁾ Comma inserito dall'art. 2, comma 3, d.lg. 26 febbraio 1999, n. 51.

¹⁹⁾ Comma così modificato dall'art. 2, comma 4, d.lg. 26 febbraio 1999, n. 51.

²⁰⁾ Comma aggiunto dall'art. 2, comma 5, d.lg. 26 febbraio 1999, n. 51.

Art. 35.***(Trattamento illecito di dati personali)***

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 11, 20 e 27, è punito con la reclusione sino a due anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, comunica o diffonde dati personali in violazione di quanto disposto dagli articoli 21, 22, 23 e 24, ovvero del divieto di cui all'articolo 28, comma 3, è punito con la reclusione da tre mesi a due anni.

3. Se dai fatti di cui ai commi 1 e 2 deriva nocumento, la reclusione è da uno a tre anni.

Art. 36.***(Omessa adozione di misure necessarie alla sicurezza dei dati)***

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

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

Art. 37.***(Inosservanza dei provvedimenti del Garante)***

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 22, comma 2, o dell'articolo 29, commi 4 e 5, è punito con la reclusione da tre mesi a due anni.

Art. 38.***(Pena accessoria)***

1. La condanna per uno dei delitti previsti dalla presente legge importa la pubblicazione della sentenza.

Art. 39.***(Sanzioni amministrative)***

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 29, comma 4, e 32, comma 1, è punito con la sanzione amministrativa del pagamento di una somma da lire un milione a lire sei milioni.

2. La violazione delle disposizioni di cui agli articoli 10 e 23, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da lire cinquecentomila a lire tre milioni.

3. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente articolo è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni.

CAPO IX

DISPOSIZIONI TRANSITORIE E FINALI ED ABROGAZIONI

Art. 40.

(Comunicazioni al Garante)

1. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dalla presente legge e dalla legge 23 dicembre 1993, n. 547, è trasmessa, a cura della cancelleria, al Garante.

Art. 41.

(Disposizioni transitorie)

1. Fermo restando l'esercizio dei diritti di cui agli articoli 13 e 29, le disposizioni della presente legge che prescrivono il consenso dell'interessato non si applicano in riferimento ai dati personali raccolti precedentemente alla data di entrata in vigore della legge stessa, o il cui trattamento sia iniziato prima di tale data. Resta salva l'applicazione delle disposizioni relative alla comunicazione e alla diffusione dei dati previste dalla presente legge.

2. ²¹⁾ *Per i trattamenti di dati personali iniziati prima del 1 gennaio 1998, le notificazioni prescritte dagli articoli 7 e 28 sono effettuate dal 1 gennaio 1998 al 31 marzo 1998 ovvero, per i trattamenti di cui all'articolo 5 riguardanti dati diversi da quelli di cui agli articoli 22 e 24, nonché per quelli di cui all'articolo 4, comma 1, lettere c), d) ed e), dal 1 aprile 1998 al 30 giugno 1998.*

3. Le misure minime di sicurezza di cui all'articolo 15, comma 2, devono essere adottate entro il termine di sei mesi dalla data di entrata in vigore del regolamento ivi previsto. Fino al decorso di tale termine, i dati personali devono essere custoditi in maniera tale da evitare un incremento dei rischi di cui all'articolo 15, comma 1.

4. Le misure di cui all'articolo 15, comma 3, devono essere adottate entro il termine di sei mesi dalla data di entrata in vigore dei regolamenti ivi previsti.

²¹⁾ Comma così sostituito dall'art. 2 d.lg. 28 luglio 1997, n. 255.

5. ²²⁾ Nei *ventiquattro* mesi successivi alla data di entrata in vigore della presente legge, i trattamenti dei dati di cui all'articolo 22, comma 3, ad opera di soggetti pubblici, esclusi gli enti pubblici economici, e all'articolo 24, possono essere proseguiti anche in assenza delle disposizioni di legge ivi indicate, previa comunicazione al Garante.

6. In sede di prima applicazione della presente legge, fino alla elezione del Garante ai sensi dell'articolo 30, le funzioni del Garante sono svolte dal presidente dell'Autorità per l'informatica nella pubblica amministrazione, fatta eccezione per l'esame dei ricorsi di cui all'articolo 29.

7. ²³⁾ *Le disposizioni della presente legge che prevedono un'autorizzazione del Garante si applicano limitatamente alla medesima autorizzazione e fatta eccezione per la disposizione di cui all'articolo 28, comma 4, lettera g), a decorrere dal 30 novembre 1997. Le medesime disposizioni possono essere applicate dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti.*

7-bis. ²⁴⁾ *In sede di prima applicazione della presente legge, le informative e le comunicazioni di cui agli articoli 10, comma 3, e 27, comma 2, possono essere date entro il 30 novembre 1997.*

Art. 42.

(Modifiche a disposizioni vigenti)

1. L'articolo 10 della legge 1 aprile 1981, n. 121, è sostituito dal seguente:
«Art. 10. - (Controlli). - 1 ²⁵⁾. Il controllo sul Centro elaborazione dati è esercitato dal *Garante per la protezione dei dati personali*, nei modi previsti dalla legge e dai regolamenti.

2. ²⁵⁾ I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità procedente ne dà notizia al *Garante per la protezione dei dati personali*.

3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intelligibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. ²⁵⁾ Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre venti giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni

²²⁾ Comma così modificato dall'art. 1, comma 1, d.lg. 8 maggio 1998, n. 135.

²³⁾ Comma così sostituito dall'art. 4, comma 1, d.lg. 9 maggio 1997, n. 123.

²⁴⁾ Comma aggiunto dall'art. 4, comma 2, d.lg. 9 maggio 1997, n. 123.

²⁵⁾ Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al *Garante per la protezione dei dati personali*.

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi. Il tribunale provvede nei modi di cui agli articoli 737 e seguenti del codice di procedura civile.».

2. Il comma 1 dell'articolo 4 del decreto legislativo 12 febbraio 1993, n. 39, è sostituito dal seguente: «1. È istituita l'Autorità per l'informatica nella pubblica amministrazione, denominata Autorità ai fini del presente decreto; tale Autorità opera in piena autonomia e con indipendenza di giudizio e di valutazione.».

3. Il comma 1 dell'articolo 5 del decreto legislativo 12 febbraio 1993, n. 39, è sostituito dal seguente: «1. Le norme concernenti l'organizzazione ed il funzionamento dell'Autorità, l'istituzione del ruolo del personale, il relativo trattamento giuridico ed economico e l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto, anche in deroga alle disposizioni sulla contabilità generale dello Stato, sono adottate con regolamento emanato con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato, su proposta del Presidente del Consiglio dei ministri, di concerto con il Ministro del tesoro e su parere conforme dell'Autorità medesima. Il parere del Consiglio di Stato sullo schema di regolamento è reso entro trenta giorni dalla ricezione della richiesta, decorsi i quali il regolamento può comunque essere emanato. Si applica il trattamento economico previsto per il personale del Garante per l'editoria e la radiodiffusione ovvero dell'organismo che dovesse subentrare nelle relative funzioni, fermo restando il limite massimo complessivo di centocinquanta unità. Restano altresì fermi gli stanziamenti dei capitoli di cui al comma 2, così come determinati per il 1995 e tenendo conto dei limiti di incremento previsti per la categoria IV per il triennio 1996-1998.».

4. ²⁵⁾ Negli articoli 9, comma 2 e 10, comma 2, della legge 30 settembre 1993, n. 388, le parole: «Garante per la protezione dei dati» sono sostituite dalle seguenti: «*Garante per la protezione dei dati personali*».

Art. 43. (Abrogazioni)

1. Sono abrogate le disposizioni di legge o di regolamento incompatibili con la presente legge e, in particolare, il quarto comma dell'articolo 8 ed il quarto comma dell'articolo 9 della legge 1 aprile 1981, n. 121. Entro sei mesi dalla data di emanazione del decreto di cui all'articolo 33, comma 1, della presente legge, il Ministro dell'interno trasferisce all'ufficio del Garante il materiale informativo raccolto a tale data in attuazione del citato articolo 8 della legge n. 121 del 1981.

²⁵⁾ Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

2. Restano ferme le disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni, nonché, in quanto compatibili, le disposizioni della legge 5 giugno 1990, n. 135, e successive modificazioni, del decreto legislativo 6 settembre 1989, n. 322, nonché le vigenti norme in materia di accesso ai documenti amministrativi ed agli archivi di Stato. Restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

3. Per i trattamenti di cui all'articolo 4, comma 1, lettera e), della presente legge, resta fermo l'obbligo di conferimento di dati ed informazioni di cui all'articolo 6, primo comma, lettera a), della legge 1 aprile 1981, n. 121.

CAPO X

COPERTURA FINANZIARIA ED ENTRATA IN VIGORE.....

Art. 44.

(Copertura finanziaria)

1. All'onere derivante dall'attuazione della presente legge, valutato in lire 8.029 milioni per il 1997 ed in lire 12.045 milioni a decorrere dal 1998, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 1997-1999, al capitolo 6856 dello stato di previsione del Ministero del tesoro per l'anno 1997, all'uopo utilizzando per il 1997, quanto a lire 4.553 milioni, l'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 3.476 milioni, l'accantonamento riguardante la Presidenza del Consiglio dei ministri e, per gli anni 1998 e 1999, quanto a lire 6.830 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 5.215 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante la Presidenza del Consiglio dei ministri.

2. Il Ministro del tesoro è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 45.

(Entrata in vigore)

1. La presente legge entra in vigore centoventi giorni dopo la sua pubblicazione nella *Gazzetta Ufficiale*. Per i trattamenti svolti senza l'ausilio di mezzi elettronici o comunque automatizzati che non riguardano taluno dei dati di cui agli articoli 22 e 24, le disposizioni della presente legge si applicano a decorrere dal 1 gennaio 1998. Fermo restando quanto previsto dall'articolo 9, comma 2, della legge 30 settembre 1993, n. 388, la presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*, limitatamente ai trattamenti di dati effettuati in esecuzione dell'accordo di cui all'articolo 4, comma 1, lettera a) e alla nomina del Garante.

5.2 LEGGE N. 676 DEL 31 DICEMBRE 1996

LEGGE 31 dicembre 1996, n. 676

Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali.²⁶⁾

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

la seguente legge:

Art. 1.

(Delega per l'emanazione di disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali)

1²⁷⁾ Il Governo della Repubblica è delegato ad emanare, entro diciotto mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, con l'osservanza dei seguenti principi e criteri direttivi:

a) specificare le modalità di trattamento dei dati personali utilizzati a fini storici, di ricerca e di statistica, tenendo conto dei principi contenuti nella Raccomandazione n. R (83) 10, adottata il 23 settembre 1983 dal Consiglio d'Europa, e successive modificazioni, con particolare riferimento alla durata della loro conservazione ed alle garanzie adeguate prescritte dalla normativa comunitaria riguardo ai dati raccolti per scopi diversi da quelli statistici, storici o scientifici e successivamente conservati per tali, diverse, finalità;

b) garantire la piena attuazione dei principi previsti dalla legislazione in materia di dati personali nell'ambito dei diversi settori di attività, nel rispetto dei criteri direttivi e dei principi della normativa comunitaria e delle seguenti raccomandazioni adottate dal Consiglio d'Europa:

1) n. R. (81) 1, del 23 gennaio 1981, in materia di dati sanitari, e successive modificazioni;

2) n. R. (85) 20, del 25 ottobre 1985, sui dati utilizzati per fini di *direct marketing*;

3) n. R. (86) 1, del 23 gennaio 1986, sui dati impiegati per scopi di sicurezza sociale;

4) n. R. (89) 2, del 18 gennaio 1989, sui dati utilizzati per finalità di lavoro;

5) n. R. (90) 19, del 13 settembre 1990, in materia di dati personali utilizzati per finalità di pagamento e di altre operazioni connesse;

²⁶⁾ L'art. 1, comma 1, della legge 6 ottobre 1998, n. 344, prevede che «I decreti legislativi previsti dagli articoli 1 e 2 della legge 31 dicembre 1996, n. 676, e successive modificazioni, in materia di trattamento dei dati personali, sono emanati entro il 31 luglio 1999, sulla base dei principi e dei criteri direttivi indicati nella medesima legge.»

²⁷⁾ Comma così modificato dall'art. 5, comma 2, d.lg. 9 maggio 1997, n. 123.

6) n. R. (91) 10, del 9 settembre 1991, sulla comunicazione a terzi dei dati personali detenuti da organi pubblici;

7) n. R. (95) 4, del 7 febbraio 1995, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici;

c) razionalizzare il trattamento economico del personale del *Garante per la protezione dei dati personali* in relazione a quello previsto dall'ordinamento per ogni altra Autorità di garanzia secondo il tendenziale criterio dell'uniformità a parità di responsabilità costituzionale;

d) individuare i presupposti per l'attribuzione di un numero di identificazione personale, ivi compreso il codice fiscale, e per il trattamento del medesimo e delle informazioni ad esso connesse, nonché per il collegamento con altri dati, sentita l'Autorità per l'informatica nella pubblica amministrazione, prevedendo adeguate garanzie con riferimento ai numeri di identificazione personale connessi a dati di carattere sensibile o idonei a rivelare i provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3 del codice di procedura penale;

e) stabilire le modalità e i termini per l'aggiornamento, per la rettificazione e per le altre modificazioni dei dati effettuati in conseguenza dell'esercizio dei diritti dell'interessato o di un provvedimento del *Garante per la protezione dei dati personali*, quando i dati personali sono riprodotti su disco ottico;

f) prevedere forme semplificate di notificazione del trattamento dei dati personali e del loro trasferimento all'estero, con particolare riguardo ai trattamenti non automatizzati di dati diversi da quelli sensibili e da quelli di cui all'articolo 686 del codice di procedura penale, ed ulteriori casi di esonero dal relativo obbligo per trattamenti da individuare preventivamente che, in ragione delle relative modalità o della natura dei dati personali, non presentino rischi di un danno all'interessato, ferma restando l'applicabilità delle altre disposizioni di legge;

g) prevedere forme di semplificazione degli adempimenti a carico delle piccole imprese e di coloro che esercitano imprese artigiane;

h) estendere l'applicazione delle disposizioni relative al trattamento dei dati da parte di chi esercita la professione di giornalista, ad eccezione delle disposizioni concernenti i dati sensibili, ai soggetti che esercitano con carattere di continuità l'attività di pubblicista o di praticante giornalistica iscritti, rispettivamente, negli elenchi di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69;

i) adattare, ai trattamenti in ambito pubblico esclusi dall'applicazione della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, i principi desumibili dalla medesima legislazione, sulla base dei seguenti criteri:

1) pieno recepimento dei principi medesimi;

2) rispetto dei principi stabiliti dalla Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, nonché della normativa comunitaria, tenendo conto dei criteri di cui alla raccomandazione n. R. (87) 15, adottata il 17 settembre 1987 dal Consiglio d'Europa;

3) ricognizione puntuale dei soggetti pubblici titolari dei trattamenti esclusi, nonché dei medesimi trattamenti;

4) introduzione degli adattamenti resi indispensabili dalla specificità degli interessi perseguiti dai suddetti trattamenti in ambito pubblico;

5) particolare considerazione per i trattamenti di dati che implicino maggiori rischi di un danno all'interessato;

6) specificazione delle modalità attraverso le quali si svolge il controllo sul rispetto delle disposizioni di legge che presiedono ai suddetti trattamenti in ambito pubblico;

l) prevedere norme che favoriscano lo sviluppo dell'informatica giuridica e le modalità di collegamento, per l'autorità giudiziaria e per l'autorità di pubblica sicurezza, con le banche dati della pubblica amministrazione;

m) mantenere il raccordo tra le attività del *Garante per la protezione dei dati personali* e quelle dell'Autorità per l'informatica nella pubblica amministrazione, anche modificando le disposizioni della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e del decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni, nonché l'armonizzazione dello stato giuridico del relativo personale;

n) stabilire le modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti i servizi accessibili al pubblico e la corrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale;

o) individuare i casi in cui, all'atto della comunicazione o della diffusione di dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da pubbliche amministrazioni, debba essere indicata la fonte di acquisizione dei dati.

Art. 2.

(Delega per l'emanazione di disposizioni correttive della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali)

1²⁸⁾ Il Governo della Repubblica è delegato ad emanare, entro diciotto mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni correttive della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, con l'osservanza dei seguenti principi e criteri direttivi:

a) rispetto dei principi e della impostazione sistematica della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

b) introduzione delle sole correzioni a tale legislazione che, dopo il primo periodo di applicazione della medesima, sentiti il *Garante per la protezione dei dati personali* e nelle materie di sua competenza l'Autorità per l'informatica nella pubblica amministrazione, si dimostrino necessarie per realizzarne pienamente i principi o per assicurarne la migliore attuazione o per adeguarla all'evoluzione tecnica del settore.

Art. 3.

(Esercizio della delega)

1. I decreti legislativi di cui agli articoli 1 e 2 sono adottati ai sensi dell'articolo 14 della legge 23 agosto 1988, n. 400.

²⁸⁾ Comma così modificato dall'art. 5, comma 2, d.lg. 9 maggio 1997, n. 123.

5.3 d.P.R. N. 501 DEL 31 MARZO 1998

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 31 marzo 1998, n. 501.

Regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'articolo 33, comma 3, della legge 31 dicembre 1996, n. 675.

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87, quinto comma, della Costituzione;

Visto l'articolo 33 della legge 31 dicembre 1996, n. 675, recante tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Ritenuto che, ai sensi del comma 3 del citato articolo 33 della legge n. 675 del 1996, con regolamento da adottare entro tre mesi dalla data di entrata in vigore della predetta legge, devono essere emanate norme concernenti l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, nonché la riscossione dei diritti di segreteria e la gestione delle spese, anche in deroga alle disposizioni sulla contabilità generale dello Stato;

Ritenuto che, ai sensi del citato comma 3 dell'articolo 33 della legge n. 675 del 1996, devono essere previste le norme concernenti il procedimento dinanzi al Garante di cui all'articolo 29, commi da 1 a 5, della medesima legge, secondo modalità tali da assicurare, nella speditezza del procedimento medesimo, il pieno rispetto del contraddittorio tra le parti interessate, nonché le norme volte a precisare le modalità per l'esercizio dei diritti di cui all'articolo 13 della legge stessa e per l'invio della notificazione dei trattamenti di dati personali per via telematica o mediante supporto magnetico o lettera raccomandata con avviso di ricevimento o con altro idoneo sistema;

Considerato che il regolamento deve disciplinare ulteriori aspetti riguardanti, tra l'altro, l'inoltro della notificazione per il tramite delle camere di commercio, industria, artigianato e agricoltura, la misura del contributo spese per l'accesso ai dati personali, la determinazione delle indennità di funzione del presidente e dei componenti del Garante, le modalità di svolgimento degli accessi alle banche di dati, delle ispezioni e delle verifiche, nonché la custodia di determinati atti e documenti, ai sensi, rispettivamente, degli articoli 7, comma 5, 13, comma 2, 30, comma 6, e 32, commi 3 e 7, della legge n. 675 del 1996;

Visto l'articolo 17, comma 1, lettera b), della legge 23 agosto 1988, n. 400;

Udito il parere del Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 17 novembre 1997;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 19 dicembre 1997;

Sulla proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri di grazia e giustizia, del tesoro, del bilancio e della programmazione economica e dell'interno;

E M A N A

il seguente regolamento:

CAPO I

IL GARANTE

Art. 1.

Definizioni

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata «legge». Ai medesimi fini, si intende, altresì:

- a) per «presidente», il presidente del Garante per la protezione dei dati personali;
- b) per «componenti», i componenti del Garante per la protezione dei dati personali;
- c) per «Ufficio», l'Ufficio del Garante per la protezione dei dati personali.

Art. 2.

G a r a n t e

1. Il Garante:

- a) determina gli indirizzi e i criteri generali della propria attività;
- b) nomina, su proposta del presidente, il segretario generale;
- c) definisce gli obiettivi ed i programmi da attuare da parte del segretario generale, indica le priorità ed emana le conseguenti direttive generali per l'azione amministrativa e per la gestione;
- d) assolve ad ogni altro compito previsto dalle leggi e dai regolamenti.

Art. 3.

Presidente e componenti

1. Il presidente è eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età.

2. Il presidente rappresenta il Garante, e sulla base degli indirizzi e dei criteri generali di cui all'articolo 2, comma 1, lettera a):

- a) designa i componenti preposti alla cura di singole questioni;
- b) convoca le riunioni del Garante, ne stabilisce l'ordine del giorno, designa i relatori e dirige i lavori;
- c) coordina i rapporti del Garante con il Parlamento e con gli altri organi costituzionali o di rilievo costituzionale, e sovrintende alle relazioni con le autorità indipendenti e di vigilanza, con le pubbliche amministrazioni, con le autorità di controllo degli altri Paesi, con gli organi dell'Unione europea e del Consiglio d'Europa e con altri organismi internazionali;
- d) promuove e resiste alle liti e ha il potere di conciliare e di transigere.

3. Il Garante nomina un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. Il presidente può delegare temporaneamente singole funzioni ad uno dei componenti.

5. I componenti curano i rapporti di cui al comma 2, lettera c), del presente articolo, in base alle decisioni del Garante.

Art. 4.

Insediamiento dell'organo e cessazione dei componenti

1. I componenti dichiarano formalmente, all'atto dell'accettazione della nomina, di non trovarsi in alcuna delle situazioni di cui all'articolo 30, comma 4, della legge.

2. Se ricorre in ogni tempo taluna delle situazioni di incompatibilità di cui all'articolo 30, comma 4, della legge, il Garante stabilisce un termine entro il quale l'interessato deve far cessare la situazione di incompatibilità. La deliberazione è adottata con l'astensione dell'interessato.

3. Decorso il termine di cui al comma 2, ove non sia cessata la situazione di incompatibilità, il Garante dichiara la decadenza del componente ai sensi dell'articolo 30, comma 4, della legge.

4. La durata in carica del componente decorre dalla data di accettazione della nomina.

5. I componenti cessano dalla carica, oltre che nell'ipotesi di cui al comma 3, per dimissioni volontarie o per impossibilità a svolgere la propria attività a causa di un impedimento di natura permanente o comunque superiore a sei mesi.

6. Le dimissioni dei componenti hanno effetto dalla data di comunicazione della loro accettazione da parte del Garante. L'impedimento permanente di cui al comma che precede è accertato dal Garante.

7. Nei casi di cui ai commi 3 e 5, il presidente o chi ne fa le veci informa immediatamente i Presidenti della Camera dei deputati e del Senato della Repubblica per l'elezione del nuovo componente.

Art. 5.

Riunioni

1. Il Garante ha sede in Roma e si riunisce nel luogo indicato nell'atto di convocazione. Le riunioni possono essere tenute in videoconferenza.

2. L'ordine del giorno è comunicato ai componenti entro il secondo giorno che precede la riunione. Nei casi d'urgenza, la convocazione può essere immediata. Durante le riunioni, l'ordine del giorno può essere integrato, previa comunicazione immediata agli assenti, se nessuno dei presenti si oppone.

3. Ciascun componente, indicandone le ragioni, può chiedere la convocazione del Garante e l'iscrizione di un argomento all'ordine del giorno. Se la richiesta proviene da almeno due componenti, il presidente la accoglie in ogni caso.

4. Salvi i casi di urgenza, la competente struttura predispone la documentazione utile entro il quinto giorno antecedente alla riunione, e sottopone al segretario generale lo schema delle osservazioni dell'Ufficio. Le osservazioni e la relativa documentazione sono formate anche mediante strumenti informatici e telematici e poste senza ritardo a disposizione del presidente e dei componenti, unitamente agli eventuali aggiornamenti.

5. Per la validità delle riunioni del Garante è necessaria la presenza del presidente e di due componenti, ovvero di tre componenti. Le deliberazioni sono adottate a maggioranza dei votanti. Il voto è sempre palese, salvo nel caso di deliberazioni concernenti il presidente o i componenti, le persone addette all'Ufficio o i consulenti.

6. Il segretario generale svolge le funzioni di segretario. Il presidente può chiamare il segretario generale o altro funzionario a riferire su singole questioni.

7. Le deliberazioni, siglate dal relatore, sono sottoscritte dal presidente e dal segretario generale.

8. Nei casi di particolare urgenza e di indifferibilità che non permettono la convocazione in tempo utile del Garante, il presidente può adottare i provvedimenti di competenza dell'organo, i quali cessano di avere efficacia sin dal momento della loro adozione se non sono ratificati dal Garante nella prima riunione utile, da convocarsi non oltre il trentesimo giorno.

9. La disposizione di cui al comma 8 non si applica in caso di esame dei ricorsi, di applicazione di sanzioni amministrative o di adozione dei divieti di cui agli articoli 21, comma 3, e 31, comma 1, lettera l), della legge, di approvazione del documento programmatico di cui all'articolo 24 e del rendiconto, ovvero allorché occorre disporre accertamenti relativamente ai trattamenti di cui all'articolo 4 della legge.

Art. 6.

Indennità e rimborsi

1. Al presidente compete un'indennità di funzione pari alla retribuzione (*segue la parola «complessiva», non ammessa al «Visto» della Corte dei conti*) in godimento al primo presidente della Corte di cassazione. L'indennità per i componenti è pari ai due terzi di quella spettante al presidente.

2. Al presidente ed ai componenti compete, qualora non siano residenti a Roma, il rimborso delle spese di viaggio e soggiorno.

CAPO II

L'UFFICIO

Art. 7.

Il segretario generale

1. All'Ufficio è preposto il segretario generale che è nominato per un quadriennio. La nomina può essere rinnovata alla scadenza.

2. Il segretario generale sovrintende al funzionamento delle strutture e vigila affinché l'attività dell'Ufficio sia svolta secondo gli obiettivi, i programmi, le priorità e le direttive generali per l'azione amministrativa e per la gestione definiti dal Garante. A tal fine:

a) verifica la completezza della documentazione predisposta per le riunioni del Garante e formula le osservazioni dell'Ufficio;

- b) cura l'esecuzione delle deliberazioni del Garante;
- c) coordina l'attività dei responsabili delle strutture e può sostituirsi ad essi in caso di inottemperanza alle direttive impartite; vigila sull'osservanza delle norme e delle disposizioni di servizio ad esso applicabili; promuove riunioni periodiche del personale, ai fini di una reciproca informativa circa il lavoro svolto;
- d) esercita, secondo i criteri e i limiti fissati nel presente regolamento, i poteri di spesa nell'ambito degli stanziamenti di bilancio;
- e) coordina la partecipazione del personale dell'Ufficio a gruppi di lavoro e a comitati, adotta gli atti opportuni per assicurare che l'Ufficio operi, di regola, mediante strumenti informatici e telematici.

Art. 8.

Organizzazione interna

1. (Precedono le parole «Con il regolamento interno», non ammesse al «Visto» della Corte dei conti) il Garante definisce l'organizzazione dell'Ufficio secondo i seguenti criteri:

- a) determinare le competenze di ciascuna struttura sulla base della omogeneità e della organicità delle funzioni;
- b) garantire la speditezza della azione amministrativa, evitando la frammentazione di procedure e favorendo il coordinamento delle strutture;
- c) organizzare le strutture secondo criteri di flessibilità per consentire sia lo svolgimento dei compiti permanenti, sia il perseguimento di specifici obiettivi anche mediante la utilizzazione di professionalità esterne nei modi di cui all'articolo 33, comma 4, della legge.

2. (Comma non ammesso al «Visto» della Corte dei conti).

Art. 9.

(Articolo non ammesso al «Visto» della Corte dei conti)

Art. 10.

Custodia degli atti riservati

1. Con provvedimento del Garante è istituita una segreteria di sicurezza presso la quale sono conservati gli atti e i documenti acquisiti ai sensi dell'articolo 32, commi 6 e 7, della legge. Alla segreteria è preposto il segretario generale e un numero di addetti all'Ufficio non superiore a cinque unità, assegnati tenendo conto del profilo professionale e delle specifiche attitudini. L'accesso agli atti e ai documenti relativi ai trattamenti di cui all'articolo 4, comma 1, lettera b), della legge è regolato dal Garante in conformità ai criteri ossevati per le segreterie di sicurezza presso le amministrazioni dello Stato.

Art. 11.

Diritti di segreteria

1. Il Garante stabilisce con proprio provvedimento l'ammontare dei diritti di segreteria inerenti ai ricorsi, alle richieste di autorizzazione e alle notificazioni, tenendo eventualmente conto anche dei relativi costi di gestione, nonché le mo-

dalità del loro pagamento, tenendo conto del disposto dell'articolo 12. Per la riscossione coattiva si applicano le disposizioni di cui al regio decreto 14 aprile 1910, n. 639, e successive modificazioni ed integrazioni.

CAPO III

REGISTRO GENERALE DEI TRATTAMENTI

Art. 12.

Notificazioni

1. Le notificazioni previste dalla legge sono effettuate, di regola, su supporto informatico, utilizzando modelli conformi allo schema predisposto dal Garante. Il Garante favorisce la disponibilità dei modelli, in particolare presso i pubblici esercizi, anche sulla base di convenzioni stipulate dal Garante con enti, associazioni di categoria e privati. Una volta predisposta, la notificazione su supporto informatico è sottoscritta dal titolare e dal responsabile anche sul supporto cartaceo sul quale deve essere riprodotta. Entrambi i supporti sono trasmessi al Garante mediante unica lettera raccomandata con avviso di ricevimento o consegna a mani proprie nell'Ufficio.

2. Successivamente alla data di entrata in vigore dei regolamenti previsti dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, il Garante individua la data a decorrere dalla quale la notificazione può essere effettuata anche per via telematica, sulla base dei modelli di cui al comma 1 resi disponibili anche mediante strumenti telematici. La notificazione è trasmessa mediante un servizio di posta elettronica o altro servizio indicato dal Garante, idoneo ad accertare l'avvenuta ricezione della notificazione anche per mezzo di un messaggio di conferma.

3. La notificazione è effettuata avvalendosi dei modelli di cui al comma 1 anche quando è redatta su supporto cartaceo, ed è trasmessa al Garante mediante lettera raccomandata con avviso di ricevimento o mediante consegna a mani proprie nell'Ufficio.

4. Anche quando il titolare effettua la notificazione con l'assistenza delle rappresentanze di categoria dei piccoli imprenditori e degli artigiani, ovvero di ordini professionali, oppure per il tramite delle camere di commercio, industria, artigianato e agricoltura, la notifica si considera avvenuta:

a) nei casi di cui ai commi 1 e 3, nel giorno indicato nell'avviso di ricevimento o nella ricevuta rilasciata dall'Ufficio;

b) nel caso di cui al comma 2, nel giorno della avvenuta ricezione.

5. La notificazione può essere effettuata per il tramite delle camere di commercio, industria, artigianato e agricoltura ai sensi dell'articolo 7, comma 5, della legge, sulla base dei modelli predisposti dal Garante tenendo conto della modulistica approvata con decreto del Ministro dell'industria, commercio, artigianato e agricoltura 7 febbraio 1996, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana 14 febbraio 1996, n. 37, supplemento ordinario n. 27. Anche in tal caso la notifica si intende avvenuta nel giorno di ricezione da parte dell'Ufficio.

6. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento all'evoluzione delle nuove tecnologie.

7. Nell'individuare l'ammontare dei diritti di segreteria per la notificazione il Garante tiene conto anche delle forme semplificate introdotte in attuazione dell'articolo 1, comma 1, lettera f), della legge 31 dicembre 1996, n. 676. I medesimi diritti:

a) sono corrisposti mediante versamento diretto o postale nei casi di cui ai commi 1 e 3;

b) sono ridotti della metà nel caso di cui al comma 2;

c) nel caso di cui al comma 5, sono versati secondo le modalità stabilite dal predetto provvedimento, con il quale è individuato anche il rimborso spese forfettario alle camere di commercio, industria, artigianato e agricoltura.

Art. 13.

Tenuta e consultazione del registro

1. Il Garante istituisce il registro generale di cui all'articolo 31 della legge, e vi include le notizie inserite nelle notificazioni ricevute.

2. Il registro è accessibile gratuitamente a chiunque senza particolari formalità, presso l'Ufficio ovvero mediante terminale ai sensi dell'articolo 31, comma 3, della legge. Il Garante può autorizzare altre forme di consultazione per via telematica, e può effettuare ricerche qualora il tenore della richiesta permetta di risalire agevolmente alle notizie oggetto di interesse.

3. Il Garante può individuare limiti e modalità per la consultazione relativa alla descrizione generale concernente le misure di sicurezza indicate nella notificazione.

4. I dati estratti in sede di consultazione possono essere trattati unicamente per finalità di applicazione della normativa in materia di protezione dei dati.

5. Il materiale informativo trasferito al Garante ai sensi dell'articolo 43, comma 1, della legge è utilizzato per le opportune verifiche e successivamente archiviato o distrutto in base alla normativa vigente.

CAPO IV

AUTORIZZAZIONI, ACCERTAMENTI E DIVIETI

Art. 14.

Autorizzazioni

1. I provvedimenti del Garante che anche su richiesta autorizzano il trattamento di dati relativamente a determinate categorie di titolari o di trattamenti sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana. Il Garante ne cura la conoscenza tra il pubblico ai sensi dell'articolo 31 della legge.

2. Nel caso in cui una richiesta di autorizzazione riguardi un trattamento che è oggetto di un provvedimento adottato ai sensi del comma 1, il Garante può provvedere comunque sulla richiesta qualora le specifiche modalità del trattamento lo giustifichino.

3. La richiesta di autorizzazione è trasmessa al Garante nei modi di cui all'articolo 12 ovvero mediante telefax, utilizzando il modello predisposto e reso disponibile dal Garante. L'autorizzazione può essere rilasciata anche mediante telefax.

4. Qualora il richiedente sia stato invitato dal Garante o dall'Ufficio a fornire informazioni o ad esibire documenti, il termine di trenta giorni di cui all'articolo 22, comma 2, della legge decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

6. *(Comma non ammesso al «Visto» della Corte dei conti).*

Art. 15. Accertamenti

1. Qualora vi sia l'assenso scritto ed informato del titolare o del responsabile, gli accertamenti di cui all'articolo 32, comma 2, della legge possono essere eseguiti anche senza l'autorizzazione di cui al comma 3 del medesimo articolo.

2. Gli accessi alle banche dati, le ispezioni e le verifiche di cui all'articolo 32 della legge effettuati presso il titolare o il responsabile sono eseguiti dandone informazione al responsabile o, se questo è assente o non è designato, agli incaricati del trattamento.

3. Salvo che per i trattamenti di cui all'articolo 4 della legge, l'autorizzazione di cui all'articolo 32, comma 3, della legge può essere richiesta anche dal presidente ai sensi dell'articolo 5, comma 8.

4. Salvo sia diversamente disposto nel decreto di autorizzazione di cui all'articolo 32, comma 3, della legge, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso qualora ciò possa facilitarne l'esecuzione.

5. I soggetti interessati, ai quali è consegnata copia dell'autorizzazione del presidente del tribunale, devono prestare la collaborazione necessaria per l'esecuzione dell'accertamento. L'accertamento è eseguito anche in caso di rifiuto e le spese in tal caso occorrenti sono poste a carico del titolare.

6. L'accertamento può essere eseguito anche dal personale dell'Ufficio munito di documento di riconoscimento, assistito, ove necessario, da consulenti ai sensi dell'articolo 33, comma 4, della legge, ovvero da altro organo dello Stato di cui il Garante si avvalga ai sensi dell'articolo 32, comma 2, della legge medesima. I soggetti predetti possono procedere a rilievi e ad operazioni tecniche e possono estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica.

7. All'accertamento possono assistere persone indicate dal titolare o dal responsabile. Dell'accesso è redatto sommario processo verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

8. Le informative, le richieste e i provvedimenti di cui al presente articolo possono essere trasmessi anche mediante telefax.

Art. 16.

Segnalazioni e divieti

1. Prima di impartire taluno dei divieti o delle segnalazioni previsti, in particolare nel caso di cui all'articolo 31, comma 1, lettere c) ed l), della legge, il Garante può invitare il titolare o il responsabile, anche in contraddittorio con gli interessati, ad effettuare il blocco.

2. I provvedimenti di divieto, quando per il numero o per la complessità degli accertamenti i destinatari non siano facilmente identificabili, sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana.

CAPO V

DIRITTI DELL'INTERESSATO

Art. 17.

Accesso ai dati personali

1. La richiesta di cui all'articolo 13, comma 1, lettera c), n. 1), della legge può essere avanzata anche per il tramite degli incaricati del trattamento, senza formalità ed anche verbalmente.

2. L'interessato deve dimostrare la propria identità, anche esibendo o allegando copia di un documento di riconoscimento. La persona che agisce su incarico dell'interessato deve inoltre esibire o allegare copia della procura o della delega recante sottoscrizione autenticata nelle forme di legge. Nei casi previsti dall'articolo 3, comma 11, della legge 15 maggio 1997, n. 127, la autenticazione non è necessaria. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica a ciò legittimata in base ai rispettivi statuti od ordinamenti.

3. La richiesta può essere trasmessa anche mediante lettera raccomandata o telefax. Si applica anche per la richiesta l'articolo 12, comma 6.

4. L'interessato può farsi assistere da una persona di fiducia.

5. Salvo che la richiesta sia riferita ad un particolare trattamento o ad una specifica banca dati, la comunicazione o il riscontro all'interessato devono comprendere tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

6. I dati sono estratti a cura del responsabile o degli incaricati del trattamento e possono essere comunicati al richiedente anche oralmente, ovvero con prospettazione mediante mezzi elettronici o comunque automatizzati, sempreché in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede in ogni caso alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

7. Qualora, a seguito della richiesta di cui all'articolo 13, comma 1, lettera c), n. 1), della legge, non risulti confermata l'esistenza di dati che riguardano l'interessato, il contributo spese che può essere richiesto non può eccedere i costi effettivamente sopportati per la ricerca effettuata nel caso specifico, e non può co-

munque superare l'importo di lire ventimila. Il contributo è determinato forfetariamente in L. 5.000 qualora i dati siano trattati con mezzi elettronici o comunque automatizzati e la risposta sia fornita in forma verbale.

8. Il contributo di cui al comma 7 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro dal quale risulta l'inesistenza dei dati e comunque non oltre cinque giorni.

9. Ai fini di una più efficace applicazione dell'articolo 13 della legge, i titolari dei trattamenti adottano le opportune misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano i singoli soggetti, tenuto conto della definizione di «dato personale» contenuta nell'articolo 1 della legge;

b) a semplificare per quanto possibile le modalità per il riscontro al richiedente e a ridurre i relativi tempi, anche nell'ambito degli uffici per le relazioni con il pubblico di cui all'articolo 12 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni.

10. Le disposizioni di cui ai commi da 1 a 6 e 9 si applicano anche agli altri casi disciplinati dall'articolo 13 della legge, nei quali, tuttavia, non è dovuto alcun contributo spese.

CAPO VI

RICORSI

Art. 18.

Presentazione e contenuto del ricorso

1. Il ricorso, ai sensi dell'articolo 29 della legge, è presentato o trasmesso al Garante a mezzo piego raccomandato o nei modi di cui all'articolo 12, comma 2, e deve contenere:

a) il nome, la denominazione o la ragione sociale e il domicilio o la residenza o la sede del ricorrente, del titolare e, ove conosciuto, del responsabile;

b) il nome dell'eventuale procuratore speciale e il domicilio eventualmente eletto;

c) l'indicazione del provvedimento richiesto, nonché della data della richiesta al responsabile ovvero del pregiudizio imminente ed irreparabile che permetta di prescindere dalla richiesta medesima;

d) gli elementi posti a fondamento della domanda;

e) la sottoscrizione del ricorrente o del procuratore speciale autenticata nelle forme di legge.

2. L'autenticazione non è richiesta qualora la sottoscrizione sia apposta presso l'Ufficio o da un procuratore speciale iscritto all'albo degli avvocati e al quale la procura sia stata conferita ai sensi dell'articolo 83 del codice di procedura civile. L'autenticazione non è richiesta qualora il ricorso sia trasmesso mediante taluno dei servizi di cui all'articolo 12, comma 2, a partire dalla data ivi indicata.

3. Al ricorso sono allegate l'eventuale procura, la copia della richiesta avanzata al responsabile e la prova del versamento dei diritti di segreteria.

4. Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione, nonché l'indicazione di un recapito che permetta di inviare comunicazioni al ricorrente o al procuratore speciale anche tramite telefax, telefono o indirizzo di posta elettronica.

5. Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso.

Art. 19.

Inammissibilità

1. Il ricorso è dichiarato inammissibile:

- a) quando proviene da un soggetto non legittimato;
- b) nei casi previsti dall'articolo 29, commi 1 e 2, della legge;
- c) qualora difetti di taluno degli elementi indicati nell'articolo 18, commi 1 e 3, salvo che il ricorrente o il procuratore speciale non lo abbiano regolarizzato, anche su invito dell'Ufficio ai sensi del comma 5 dell'articolo 18, entro tre giorni dalla data della sua presentazione o della ricezione dell'invito. In tal caso, il ricorso si considera presentato all'atto della regolarizzazione.

Art. 20.

Procedimento

1. Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato a cura dell'Ufficio al titolare e al responsabile, con l'avvertimento della facoltà di aderirvi spontaneamente entro tre giorni dalla sua comunicazione.

2. In caso di adesione spontanea, è dichiarato il non luogo a provvedere. Nel medesimo caso, se vi è stata previa richiesta del ricorrente, l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte, è determinato in misura forfettaria.

3. La comunicazione di cui al comma 1 è trasmessa anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio, anche dal relatore o dal responsabile del procedimento o mediante videoconferenza.

4. Il provvedimento che dispone una perizia ai sensi dell'articolo 29, comma 3, della legge precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti, le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.

5. Nel procedimento, il titolare e il responsabile possono essere assistiti da un procuratore o da altra persona di fiducia.

6. Il provvedimento anche provvisorio o di rigetto adottato dal Garante è comunicato alle parti entro tre giorni presso il domicilio eletto o, in mancanza, presso quello indicato nel ricorso o nelle memorie.

7. Il provvedimento di cui all'articolo 29, comma 5, della legge può essere adottato anche prima della comunicazione di cui al comma 1 del presente articolo.

8. Se vi è l'assenso delle parti, il termine di cui all'articolo 29, commi 4 e 5, della legge può essere prorogato per un periodo non superiore ad ulteriori venti giorni.

9. Se vi è stata previa richiesta di taluna delle parti, il provvedimento espresso che definisce il procedimento determina in misura forfettaria l'ammon-tare delle spese e dei diritti inerenti al ricorso posti a carico, anche in parte, del soccombente.

10. I provvedimenti di accoglimento o di rigetto sono pubblicati ai sensi dell'articolo 21 previa omissione, anche a richiesta dell'interessato, delle relative generalità. I medesimi provvedimenti possono essere comunicati alle parti anche mediante telefax.

11. Qualora sorgano difficoltà o contestazioni riguardo all'esecuzione del provvedimento di cui all'articolo 29, commi 4 e 5, della legge, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, ove necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

CAPO VII

DISPOSIZIONI VARIE

Art. 21.

Bollettino e quesiti

1. Il Garante promuove la pubblicazione di un Bollettino nel quale sono riportati, previa omissione, anche a richiesta dell'interessato, delle relative generalità, i provvedimenti più significativi, gli atti e i documenti di cui si ritiene opportuna la pubblicità, e le risposte di interesse generale date ai quesiti pervenuti;

2. Il Bollettino può essere edito anche attraverso strumenti telematici.

3. Il Garante cura la catalogazione dei provvedimenti di cui all'articolo 40 della legge, in particolare mediante il Bollettino, e ne agevola la consultazione anche da parte degli uffici giudiziari.

Art. 22.

Rappresentanza e difesa

1. Fermo restando quanto previsto dall'articolo 23 della legge 24 novembre 1981, n. 689, la rappresentanza e la difesa in giudizio del Garante è assunta dall'Avvocatura dello Stato ai sensi dell'articolo 43 del regio decreto 30 settembre 1933, n. 1611, e successive modificazioni ed integrazioni, recante il testo unico delle leggi e delle norme giuridiche sulla rappresentanza e difesa in giudizio dello Stato e sull'ordinamento dell'Avvocatura dello Stato.

CAPO VIII

GESTIONE DELLE SPESE

Art. 23.

Contabilità speciale

1. Alle spese di funzionamento del Garante, ivi comprese quelle dell'Ufficio, si provvede mediante apertura di una contabilità speciale presso la sezione di tesoreria provinciale dello Stato di Roma, intestata al Garante.

2. La contabilità speciale è alimentata mediante mandati, commutabili in quietanze di entrata della stessa contabilità speciale, tratti sul fondo di cui all'articolo 33, comma 2, della legge.

3. Alla contabilità speciale di cui al comma 1 affluiscono anche le somme corrisposte a titolo di pagamento dei diritti di segreteria di cui all'articolo 33, comma 3, della legge o a qualunque altro titolo in base alle leggi e ai regolamenti.

4. Il Garante può stipulare apposita convenzione con soggetti pubblici e privati, al fine di disciplinare, sulla base di criteri di semplicità e di speditezza, le modalità di versamento delle somme di cui al comma 3.

Art. 24.

Programmazione finanziaria

1. Le spese sono disposte sulla base di un documento programmatico che fissa, all'inizio di ogni esercizio, gli obiettivi da raggiungere e i criteri di massima da osservare nello svolgimento dell'attività istituzionale.

Art. 25.

Spese e pagamenti per beni e servizi

1. Salvo quanto disposto nei successivi articoli in materia di procedure contrattuali, le iniziative di spesa per la fornitura di beni e servizi sono deliberate dal Garante o, sulla base dei criteri stabiliti dal Garante, dal presidente.

2. Alle spese di cui al comma 1 provvede il presidente o, per sua delega, il segretario generale, sulla base dei criteri stabiliti dal Garante.

Art. 26.

P a g a m e n t i

1. I pagamenti da imputarsi alla contabilità speciale sono disposti dal presidente o, per sua delega, dal segretario generale o da altro dirigente.

2. Sugli ordini di pagamento emessi dal presidente, dal segretario generale o dal dirigente di cui al comma 1, è apposto, prima dell'esecuzione, il visto del responsabile del servizio amministrazione e contabilità.

Art. 27.***Conservazione delle somme***

1. Le somme versate sulla contabilità speciale non erogate alla chiusura dell'esercizio finanziario possono essere conservate per effettuare i pagamenti fino al termine dell'esercizio successivo. Alla chiusura di tale esercizio il Garante può individuare le somme relative a programmi già deliberati che possono essere ulteriormente conservate per il biennio successivo.

Art. 28.***Spese per i servizi in economia***

1. Per le spese occorrenti all'affitto e alla manutenzione dei locali, all'acquisto e alla manutenzione di mobili, arredi e impianti tecnici e per ogni altra spesa necessaria ai servizi dell'economato, il presidente può autorizzare l'econo-mo-cassiere ad effettuare spese di importo non superiore a lire dieci milioni, ai migliori prezzi correnti.

2. Gli assuntori e i fornitori devono prestare, se richiesti, idonea cauzione.

3. Per quanto non disposto dal presente regolamento, alle spese di cui al comma 1 si applicano, in quanto compatibili, le disposizioni del regolamento per i servizi in economia della Presidenza del Consiglio dei Ministri, approvato con decreto del Presidente della Repubblica 5 giugno 1985, n. 359, e successive modificazioni ed integrazioni.

Art. 29.***Servizio di cassa interno***

1. Il presidente può autorizzare, previa determinazione del Garante, l'istituzione di un servizio di cassa interno. L'incarico di economo-cassiere è conferito, su proposta del segretario generale, ad un dipendente in servizio presso il Garante, per un periodo non superiore a due anni. L'incarico è rinnovabile per non più di tre volte consecutive.

2. L'econo-mo-cassiere, posto funzionalmente alle dipendenze del segretario generale, può essere dotato all'inizio di ciascun anno finanziario, con determinazione del presidente, di un fondo non superiore a lire venti milioni, reintegrabile durante l'esercizio, previa presentazione del rendiconto delle somme già spese. Con tale fondo si può provvedere, di norma, al pagamento delle spese minute di ufficio, delle spese per piccole riparazioni e manutenzione di mobili e locali, delle spese postali o di vetture nonché delle spese per i trasporti e per l'acquisto di carburante, giornali e pubblicazioni periodiche.

3. Possono gravare sul fondo di cui al comma 2 gli acconti per le spese di viaggio e di indennità di missione e delle spese di rappresentanza, nonché le spese per la pubblicazione di bandi ed altri avvisi sulle *Gazzette Ufficiali*, sulla stampa quotidiana e su altri bollettini periodici, ove non sia possibile provvedervi tempestivamente con ordinativi di pagamento tratti sulla contabilità speciale.

4. Nessun pagamento può essere effettuato con il fondo a disposizione senza il visto del responsabile del servizio amministrazione e contabilità.

Art. 30.***Economo-cassiere***

1. L'economo-cassiere è responsabile delle operazioni di cassa e accerta la regolarità formale delle relative determinazioni di pagamento; è altresì responsabile del numerario e di ogni altro valore affidatogli.

2. L'economo-cassiere tiene:

a) un registro di cassa per le operazioni di entrata e di uscita dal quale risultino, giornalmente, il fondo di cassa iniziale, i pagamenti effettuati nella giornata e il fondo di cassa esistente alla chiusura della cassa;

b) un registro dei valori e dei titoli in deposito.

3. Il denaro e i valori sono custoditi in cassaforte. Non possono essere depositati in cassaforte denaro, titoli ed oggetti di valore che non siano di pertinenza degli uffici.

Art. 31.***Situazione di cassa***

1. Il responsabile del servizio di amministrazione e contabilità provvede mensilmente alla ricognizione materiale del denaro e dei valori custoditi nella cassa, sulla base della situazione di cassa compilata dall'economo-cassiere mediante apposito verbale.

Art. 32.***Inventari***

1. Dei beni acquistati o dati in uso al Garante sono redatti appositi inventari, nei quali i beni stessi sono classificati in conformità alle disposizioni vigenti per le amministrazioni dello Stato.

Art. 33.***Manutenzione dei beni***

1. L'economo-cassiere svolge le funzioni di consegnatario e provvede direttamente alla manutenzione dei beni, degli arredamenti e dei materiali in dotazione all'Ufficio; vigila, altresì, sulla regolare esecuzione dei servizi appaltati.

2. Ai fini di cui al comma 1, l'economo-cassiere tiene:

a) un registro d'inventario per i mobili e le attrezzature in dotazione all'Ufficio;

b) un registro di carico e scarico per il materiale di facile consumo.

Art. 34.***Elenco indicativo delle spese di funzionamento***

1. Sul fondo per le spese di funzionamento del Garante gravano le seguenti spese:

a) le indennità spettanti al presidente e ai componenti, nonché al segretario generale;

b) gli stipendi, le indennità e gli altri assegni fissi spettanti al personale in servizio presso l'Ufficio;

- c) i compensi per il lavoro straordinario e quelli incentivanti la produttività;
- d) i compensi ai consulenti e alle società di consulenza, (*seguono alcune parole non ammesse al «Visto» della Corte dei conti*);
- e) le indennità e i rimborsi-spese per missioni svolte anche dal presidente e dai componenti nel territorio nazionale e all'estero;
- f) le spese postali e per servizi telegrafici, telefonici e telematici, nonché le altre spese inerenti al servizio di corrispondenza;
- g) le spese di locazione, manutenzione, adattamento dei locali e dei relativi impianti, nonché per l'acquisto, il noleggio e la manutenzione di autoveicoli, carburante e lubrificante;
- h) le spese per l'acquisto e la manutenzione di mobili ed arredi, per l'acquisto, il noleggio e la manutenzione di macchine per scrivere e per calcolo, di apparecchiature telefoniche e televisive, di registrazione del suono e delle immagini, di fotoproduzione e di strumenti elettronici o comunque automatizzati;
- i) le spese per l'acquisto di libri, giornali, riviste ed altre pubblicazioni, nonché per la pubblicazione del Bollettino di cui all'articolo 21;
- l) le spese relative all'organizzazione o alla partecipazione ad incontri di studio, convegni e seminari di aggiornamento professionale, congressi, mostre ed altre manifestazioni;
- m) le spese di trasporto, imballaggio e facchinaggio;
- n) le spese casuali;
- o) le spese di rappresentanza, da effettuarsi sulla base dei criteri e delle istruzioni impartite dal Garante;
- p) le spese per interventi assistenziali nei confronti del personale;
- q) ogni altra spesa necessaria al funzionamento dell'Ufficio.

2. Per spese di rappresentanza, di cui al comma 1, lettera o), si intendono quelle finalizzate a soddisfare le esigenze del Garante e dell'Ufficio di manifestarsi all'esterno e di intrattenere pubbliche relazioni con altri soggetti nell'ambito dei propri fini istituzionali. Sono comunque da considerarsi tali:

- a) piccoli doni, quali targhe, medaglie, libri, oggetti simbolici a personalità italiane e straniere o a componenti di delegazioni straniere in visita al Garante, oppure in occasione di visite all'estero compiute da rappresentanti o delegazioni ufficiali del Garante e dell'Ufficio;
- b) omaggi floreali o necrologi;
- c) consumazioni in occasione di incontri di lavoro con personalità estranee al Garante o in occasione di visite ufficiali presso il Garante di componenti di missioni di studio italiani e stranieri.

3. Per le spese di cui al comma 1, relative all'acquisto di beni e servizi, non è richiesta l'autorizzazione del Provveditorato generale dello Stato.

Art. 35.

Rendiconto e controllo della gestione

1. Entro il 31 marzo di ciascun anno, il servizio amministrazione e contabilità predispone il rendiconto delle spese deliberate e di quelle pagate, distinte per categorie, da sottoporre all'approvazione del Garante.

2. Il rendiconto, vistato dal segretario generale, è articolato funzionalmente sulla base dei programmi e degli obiettivi indicati negli articoli 2 e 24, in modo da consentire un controllo adeguato della gestione ed una corretta programma-

zione finanziaria dell'azione del Garante. In caso di necessità, le direttive generali di cui all'articolo 2 possono essere integrate dal Garante anche in corso di esercizio.

3. Entro il 30 aprile, il rendiconto approvato, accompagnato da una relazione illustrativa del presidente, è trasmesso alla Corte dei conti per il controllo consuntivo di cui all'articolo 33, comma 2, della legge, per il tramite della Ragioneria centrale presso il Ministero del tesoro.

4. *(Comma non ammesso al «Visto» della Corte dei conti).*

Art. 36.

Norme contrattuali di carattere generale

1. Le disposizioni del presente regolamento in materia contrattuale si applicano limitatamente ai casi non disciplinati dalla normativa comunitaria e da quella nazionale di recepimento.

2. Ai lavori, agli acquisti, alle alienazioni, alle permuta, alle forniture, alle locazioni, comprese quelle finanziarie, ed ai servizi in genere si provvede con contratti da stipularsi secondo le procedure e le norme contenute nel presente regolamento.

3. I contratti sono stipulati di regola nelle forme del diritto privato, anche mediante scambio di corrispondenza secondo l'uso del commercio. La forma dei contratti è in ogni caso quella scritta.

4. Il Garante delibera ed approva i contratti. Tali poteri possono essere delegati al presidente e al segretario generale, nei limiti di valore stabiliti dal Garante.

5. I contratti devono avere termine e durata certi e non possono comunque superare, anche con successive proroghe, i nove anni, salvi i casi di assoluta necessità o convenienza da indicare nella relativa delibera di autorizzazione della spesa.

6. Salvo quanto diversamente disposto per legge, la valutazione della congruità dei prezzi è compiuta dal Garante o dai soggetti di cui al comma 4 previa acquisizione del parere di una commissione costituita con provvedimento del Garante stesso. Per lavori di particolare complessità tecnica, può essere acquisito il parere di organi tecnici delle amministrazioni dello Stato. Per i contratti di importo compresi tra i 5 milioni e i 100 milioni di lire, il Garante o i soggetti di cui al comma 4 possono acquisire un parere sulla congruità dei prezzi da parte di una commissione permanente composta prevalentemente da funzionari interni. Ai soli componenti esterni delle anzidette commissioni, se presenti, possono essere corrisposti compensi determinati di volta in volta dal presidente in rapporto alla durata e alla rilevanza delle prestazioni. Il parere di congruità non è richiesto per l'affidamento di studi, ricerche e consulenze di cui al successivo articolo 45.

7. Nei contratti sono previste adeguate penalità per inadempienze e ritardi nell'esecuzione dei lavori e delle prestazioni convenute. Nei contratti a durata pluriennale o ad esecuzione continuata o periodica, e salvo che nei casi disciplinati espressamente per legge, il Garante può riservarsi la facoltà di rinegoziare i costi a proprio favore, al verificarsi di condizioni od eventi contrattualmente predeterminati. Tale clausola è comunque prevista per l'ipotesi in cui l'originaria congruità dei prezzi, per qualsiasi motivo, venga meno.

8. Fermo restando quanto previsto per legge, l'aggiudicazione o l'affidamento di lavori di particolare complessità sono effettuati dal Garante sulla base di un progetto esecutivo recante la precisa indicazione del costo complessivo dei lavori. Il costo così definito può essere aumentato solo per causa di forza maggiore o per motivate ragioni tecniche, sempre che detti eventi fossero imprevedibili all'atto della progettazione. In tal caso, non possono essere effettuati lavori nuovi o diversi senza il preventivo assenso scritto da parte del Garante o, previa delega nel rispetto dei limiti di cui al comma 4, da parte del presidente o del segretario generale. In ogni caso l'eventuale incremento dei costi, compresa la revisione dei prezzi, è disciplinato dalle norme vigenti in materia per le amministrazioni dello Stato.

9. Oltre alle anticipazioni consentite per legge, sono ammessi pagamenti in acconto in ragione delle parti di opere realizzate, dei beni forniti e delle prestazioni eseguite. È vietata la corresponsione di interessi e provvigioni a favore dell'appaltatore o dei fornitori sulle somme eventualmente anticipate per l'esecuzione del contratto.

10. Deve essere osservato il principio della non discriminazione in base alla nazionalità nei confronti dei fornitori appartenenti agli Stati membri dell'Unione europea.

Art. 37.

Procedure contrattuali

1. Ai lavori, alle forniture e ai servizi si provvede, di norma, mediante gare disciplinate dalle successive disposizioni di cui al presente regolamento.

2. Le procedure contrattuali possono essere «aperte» (pubblico incanto), «ristrette» (licitazione privata e appalto concorso) e «negoziare» (trattativa privata).

3. Salvo che il Garante ritenga più vantaggioso il ricorso alla procedura «aperta», le gare si svolgono seguendo, di norma, la procedura «ristretta».

Art. 38.

Procedura aperta

1. Nella procedura «aperta» (pubblico incanto) possono presentare offerta tutti i soggetti interessati. I concorrenti devono documentare i requisiti di partecipazione richiesti dal bando di gara.

Art. 39.

Procedura ristretta

1. Nella procedura «ristretta» (licitazione privata e appalto concorso) sono invitati a presentare la propria offerta solo i concorrenti che, avendo presentato domanda di partecipazione alla gara, abbiano dimostrato la propria capacità tecnica, economica e finanziaria ad effettuare la prestazione richiesta. Il bando può prevedere che alcuni requisiti siano comprovati mediante autocertificazione, fermo restando l'obbligo di produrre la relativa documentazione prima dell'eventuale aggiudicazione.

2. La selezione dei concorrenti da invitare alla gara, nell'ambito di coloro che hanno presentato domanda di partecipazione, è effettuata da una commissione nominata all'uopo dal presidente, o, su sua delega, dal segretario generale. All'esito della selezione è comunque assicurata una partecipazione che consenta un'adeguata concorrenza.

3. Ai concorrenti selezionati è inviata la lettera di invito a presentare, entro termini specificati, la propria offerta tecnico-economica. Alla lettera sono allegati il capitolato tecnico e lo schema di contratto che regola il rapporto tra il Garante e l'aggiudicatario.

4. Per lo svolgimento della procedura ristretta è necessaria la presenza di almeno due offerte valide.

Art. 40.

Criteri di aggiudicazione

1. Nel bando di gara sono specificati i criteri di aggiudicazione seguiti dal Garante e che sono, alternativamente, i seguenti:

a) in caso di pubblico incanto, al prezzo più alto se si tratta di contratti attivi, ovvero al prezzo più basso se si tratta di contratti passivi;

b) in caso di licitazione privata, al prezzo più basso qualora il capitolato tecnico sia molto particolareggiato e, comunque, tale da identificare inequivocabilmente la prestazione che il Garante intende ricevere;

c) in caso di licitazione privata e di appalto concorso, all'offerta più vantaggiosa sotto il profilo tecnico-economico, qualora nel capitolato tecnico siano contenute solo prescrizioni di massima e si ritenga conveniente, quindi, avvalersi della collaborazione e dell'apporto di competenza tecnica ed esperienza specifica da parte dell'offerente per l'elaborazione del progetto definitivo. In tal caso nel bando di gara sono indicati, in ordine decrescente di importanza, gli elementi presi in considerazione per la valutazione comparativa delle offerte.

Art. 41.

Procedura negoziata

1. È ammessa la procedura negoziata (trattativa privata) nei seguenti casi:

a) quando, a seguito di esperimento di gara, per qualsiasi motivo, l'aggiudicazione non abbia avuto luogo;

b) per la fornitura di beni, la prestazione di servizi, ivi compresi quelli del settore informatico, e l'esecuzione di lavori che una sola impresa può fornire od eseguire con i requisiti tecnici ed il grado di perfezione richiesti, nonché quando l'acquisto riguardi beni la cui produzione è garantita da privativa industriale;

c) per la locazione d'immobili;

d) quando l'urgenza, adeguatamente motivata, dei lavori, degli acquisti e delle forniture dei beni e servizi dovuta a circostanze imprevedibili, o quando la particolare natura e le caratteristiche dell'oggetto e delle prestazioni anche in relazione ad esigenze di sicurezza o di segretezza dei lavori, ovvero quando la necessità di far eseguire le prestazioni a spese e a rischio degli imprenditori inadempienti, non consentano l'indugio della gara;

e) per lavori complementari non considerati nel contratto originario o che siano resi necessari da circostanze imprevedibili all'atto dell'affidamento del contratto, a condizione che siano affidati allo stesso contraente, non siano tecnicamente o economicamente separabili dalla prestazione principale, ovvero,

benché separabili, siano strettamente necessari per il completamento dei lavori o della fornitura originaria e il loro ammontare non superi il 50% dell'importo originario;

f) per l'affidamento al medesimo contraente di forniture destinate al completamento, al rinnovo parziale, o all'ampliamento di quelle esistenti, qualora il ricorso ad altri fornitori costringa ad acquistare materiale di tecnica differente, il cui impiego o la cui manutenzione comporti notevoli difficoltà o incompatibilità tecniche. La durata di tali contratti non può superare, come norma generale, i tre anni;

g) per l'acquisizione di beni o prodotti soggetti a prezzi amministrati o sorvegliati;

h) quando trattasi di contratti di importo non superiore a 200 milioni di lire, con esclusione dei casi in cui detti contratti costituiscano ripetizione, frazionamento o completamento di precedenti lavori o forniture;

i) quando trattasi di contratti di assicurazione.

2. Nei casi indicati alle lettere a), d), h) ed i) del comma 1 devono essere interpellate più imprese o ditte, persone od enti e, comunque, non inferiori a tre.

Art. 42.

Transazioni

1. Per la definizione delle transazioni di importo superiore a lire 100 milioni il presidente richiede il parere preventivo dell'Avvocatura generale dello Stato.

Art. 43.

Collaudi e verifiche

1. Tutti i lavori e le forniture sono soggetti a collaudo secondo le norme stabilite dalle vigenti disposizioni e dal contratto, il quale può prevedere collaudi parziali ed in corso d'opera.

2. Il collaudo è effettuato in forma individuale e collegiale dal personale addetto all'ufficio in possesso della competenza tecnica necessaria, ovvero, qualora se ne ravvisi la necessità, da consulenti appositamente incaricati. La nomina dei collaudatori è effettuata dal presidente per lavori e forniture d'importo superiore a lire 500 milioni ovvero in caso di nomina di consulenti, e dal segretario generale negli altri casi.

3. Il collaudo non può essere effettuato da chi abbia progettato, diretto o sorvegliato i lavori, ovvero da chi abbia partecipato all'aggiudicazione del contratto o alle relative forniture.

4. Nel caso in cui l'importo dei lavori o delle forniture non superi i 150 milioni di lire, l'atto formale di collaudo può essere sostituito da un certificato di regolare esecuzione rilasciato dal responsabile del servizio o da altro dipendente appositamente incaricato.

5. Per l'acquisizione di beni e servizi diversi dai lavori e dalle forniture di cui ai commi precedenti, relativamente ai quali non sia possibile procedere al collaudo secondo le modalità e i criteri ivi previsti, il funzionario cui viene effettuata la consegna procede ad una verifica della regolarità e della corrispondenza dei beni e dei servizi acquistati con quelli ordinati. Di tale corrispondenza e regolarità è redatta apposita attestazione.

Art. 44.***Adeguamento limiti di somma***

1. I limiti di spesa e di somma indicati nei precedenti articoli sono aggiornati annualmente, con deliberazione del Garante, in base alle variazioni dell'indice ISTAT dei prezzi al consumo.

Art. 45.***Studi, ricerche, consulenze e prestazioni professionali***

1. In sede di applicazione dell'articolo 33, comma 4, della legge, possono essere stipulati anche contratti con liberi professionisti, con dipendenti pubblici o con esperti di qualificata esperienza, nei limiti e alle condizioni previsti dalle rispettive norme di stato giuridico, con persone giuridiche pubbliche e private e con associazioni. Tali contratti, della durata massima di un anno, possono essere rinnovati per non più di tre volte.

2. I compensi per i consulenti iscritti ad albi professionali sono corrisposti, anche nei modi di cui all'articolo 28, comma 1, sulla base delle tariffe minime stabilite per le relative categorie professionali, mentre per gli altri professionisti o per i dipendenti pubblici, i compensi sono stabiliti di volta in volta dal segretario generale, in rapporto alla durata e alla rilevanza delle prestazioni, secondo i criteri stabiliti nell'apposito tariffario preventivamente approvato dal Garante, da richiamarsi nel relativo disciplinare di incarico.

Art. 46.***Norme transitorie e di rinvio***

1. In deroga a quanto previsto nell'articolo 27, per gli esercizi finanziari relativi al 1997 e al 1998, le disposizioni del medesimo articolo si applicano anche in riferimento alle somme versate sulla contabilità speciale, non deliberate dal Garante entro la chiusura di ciascun esercizio finanziario, limitatamente alle spese di cui all'articolo 34, comma 1, lettere d), g), h), i), l) ed m).

2. Per quanto non disciplinato dal presente regolamento si applicano le norme della legge e del regolamento per l'amministrazione del patrimonio e per la contabilità generale dello Stato, in quanto compatibili.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 31 marzo 1998

SCÀLFARO

PRODI, Presidente del Consiglio dei Ministri

FLICK, Ministro di grazia e giustizia

**CIAMPI, Ministro del tesoro, del bilancio
e della programmazione economica**

NAPOLITANO, Ministro dell'interno

Visto, il Guardasigilli: FLICK

5.4 CODICE ETICO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Codice etico del Garante per la protezione dei dati personali.

Art. 1.

(Finalità ed ambito di applicazione)

Il presente codice etico (di seguito denominato *codice*) reca i principi-guida del comportamento dei soggetti che operano presso il Garante per la protezione dei dati personali e specifica i doveri di lealtà, imparzialità, diligenza ed operosità previsti per i dipendenti pubblici.

L'attività di tali soggetti deve essere conforme alla posizione di indipendenza riconosciuta al Garante, ai compiti di garanzia ad esso affidati, all'imparzialità e alla trasparenza dell'attività amministrativa, nonché al rispetto degli obblighi di riservatezza.

Il codice si applica ai dipendenti che operano presso l'Ufficio del Garante anche in posizione di collocamento fuori ruolo, di comando, di distacco o a tempo parziale. Il codice si applica anche ai consulenti e alle persone autorizzate a frequentare l'Ufficio per effettuare studi o ricerche.

Art. 2.

(Disposizioni generali)

Il dipendente si impegna a rispettare il codice al momento dell'assunzione dell'incarico e a tenere una condotta ispirata ai principi di lealtà, imparzialità, integrità ed onestà.

Il dipendente evita ogni atto o comportamento che violi o possa far ritenere violate le disposizioni di legge o di regolamento o contenute nel codice.

I rapporti tra l'Ufficio e i dipendenti sono improntati a fiducia e collaborazione. Il dipendente si adopera affinché le relazioni con i colleghi siano ispirate ad armonia ed evita atti o comportamenti caratterizzati da animosità o conflittualità.

Il dipendente conforma la propria attività e l'uso dei beni dell'Ufficio ai criteri di correttezza, economicità, efficienza ed efficacia. Il dipendente dedica al lavoro d'ufficio la giusta quantità di tempo e di impegno, evitando assenze o allontanamenti indebiti.

Il dipendente limita ai casi di assoluta necessità l'eventuale uso per ragioni personali delle apparecchiature telefoniche, delle fotocopiatrici e degli elaboratori, anche in caso di ricezione di comunicazioni.

Nelle relazioni con l'esterno, il dipendente si comporta in modo tale da determinare fiducia e collaborazione da parte dei soggetti che entrano in contatto con l'Ufficio; mostra cortesia e disponibilità nella comunicazione con il pubblico e cura la trattazione delle questioni in maniera efficiente e sollecita.

Art. 3.
(Imparzialità)

Il dipendente opera con imparzialità, evita trattamenti di favore e disparità di trattamento, si astiene dall'effettuare pressioni indebite e le respinge, adotta iniziative e decisioni nella massima trasparenza ed evita di creare o di fruire di situazioni di privilegio.

Nei rapporti con i soggetti interessati a qualunque titolo all'attività del Garante, il dipendente non assume impegni né fa promesse personali che possano condizionare l'adempimento dei doveri d'ufficio.

Il dipendente, fermo il diritto di associazione e il diritto di adesione a partiti politici e sindacati, comunica al segretario generale l'adesione ad associazioni, circoli od altri organismi di qualsiasi natura i cui interessi possano influenzare lo svolgimento delle funzioni d'ufficio.

Art. 4.
(Integrità)

Il dipendente non utilizza l'Ufficio per perseguire fini o per conseguire benefici privati e personali.

Il dipendente non si avvale della posizione che ricopre nell'Ufficio per ottenere utilità o benefici nei rapporti esterni anche di natura privata. Nei rapporti privati, il dipendente evita di dichiarare o di lasciare intendere la propria posizione nei casi in cui tale menzione non risponda ad esigenze obiettive.

Il dipendente non fa uso delle informazioni non disponibili al pubblico o non rese pubbliche, ottenute anche in via confidenziale nell'attività d'ufficio, per realizzare profitti o interessi privati.

Il dipendente evita di ricevere benefici di ogni genere, anche in occasione di viaggi, seminari e convegni, che possano essere o apparire tali da influenzarne l'indipendenza di giudizio e l'imparzialità; inoltre non sollecita né accetta, per sé o per altri, alcun dono o altra utilità da parte di soggetti comunque interessati all'attività del Garante o che intendano entrare in rapporto con esso, con eccezione dei regali di modico valore.

Nei caso in cui riceva pressioni illegittime o gli vengano offerti regali, benefici o altre utilità eccedenti un modico valore, il dipendente è tenuto a darne tempestiva comunicazione al segretario generale.

Art. 5
(Norme particolari)

Fuori dell'ordinario procedimento di assegnazione delle pratiche, il dipendente non sollecita né riceve comunicazioni a lui destinate, né invia missive non autorizzate.

Il dipendente partecipa ai soli incontri e riunioni, anche informali, rilevanti per l'attività d'ufficio cui è autorizzato a prendere parte; evita inoltre contatti non autorizzati con destinatari anche indiretti degli atti e dei provvedimenti in fase di adozione o con chi fornisce o intende fornire beni o servizi all'Ufficio.

La partecipazione dei dipendenti a convegni, seminari e dibattiti è autorizzata dal segretario generale sulla base dei criteri di trasparenza, competenza, opportunità e rotazione, previa dichiarazione circa l'ammontare dell'eventuale rimborso, gettone o compenso percepito a qualunque titolo, ovvero circa la fruizione di particolari benefici.

Art. 6.
(Conflitto d'interessi)

Il dipendente si adopera per prevenire situazioni di conflitto d'interessi con l'Ufficio, ed informa il segretario generale degli eventuali interessi, anche di natura economica, che egli, il coniuge, i parenti entro il quarto grado o i soggetti conviventi abbiano nelle attività o nelle decisioni di propria competenza. Il dipendente si astiene in ogni caso dal partecipare ad attività o decisioni che determinano tale conflitto, e fornisce al segretario generale ogni ulteriore informazione richiesta.

Il dipendente si astiene dal partecipare, per un periodo di almeno due anni, alla trattazione delle questioni di competenza del Garante che possano coinvolgere interessi di propri precedenti soci in affari ovvero, fuori dei casi in cui è autorizzato, di precedenti datori di lavoro.

Il dipendente si astiene in ogni altro caso in cui sussistano gravi ragioni di convenienza o nei quali, anche in ragione di una grave inimicizia, la propria partecipazione alla trattazione della questione possa ingenerare sfiducia nell'imparzialità del Garante.

Il dipendente informa tempestivamente il segretario generale degli eventuali contatti avviati, ai fini dell'assunzione di incarichi o di attività esterni all'Ufficio, con soggetti interessati anche solo potenzialmente all'attività del Garante.

Il presente codice impegna il dipendente che cessi di prestare servizio presso l'Ufficio a non trovarsi in una situazione di conflitto di interessi con il Garante per un periodo di almeno due anni.

Art. 7.
(Riservatezza)

Il dipendente rispetta il segreto d'ufficio e mantiene riservate le notizie e le informazioni apprese nell'esercizio delle proprie funzioni e che non siano oggetto di trasparenza in conformità alla legge e ai regolamenti. Il dipendente osserva il dovere di riservatezza anche dopo la cessazione dal servizio.

In particolare, il dipendente non fornisce informazioni in merito ad attività istruttorie, ispettive o di indagine in corso presso l'Ufficio e non rilascia informazioni relative ad atti e provvedimenti prima della loro comunicazione alle parti.

Il dipendente consulta i soli atti e fascicoli ai quali è autorizzato ad accedere e ne fa un uso conforme ai doveri d'ufficio, consentendone l'accesso a coloro che ne abbiano titolo e in conformità alle prescrizioni impartite nell'Ufficio.

Il dipendente previene l'eventuale dispersione di dati osservando le misure di sicurezza impartite, custodendo con ordine e cura gli atti affidati ed evitando di effettuarne inutili copie.

Art. 8.***(Rapporti con la stampa)***

In relazione all'attività del Garante, il dipendente non intrattiene rapporti con organi di stampa o con altri mezzi di informazione e si astiene da ogni dichiarazione pubblica che possa incidere sull'immagine del Garante. Qualora sia richiesto di fornire chiarimenti o informazioni da parte degli organi di stampa o da altri mezzi di informazione, ne dà tempestiva notizia al servizio stampa.

I rapporti con la stampa e con i fornitori di informazione sono ispirati al criterio della parità di trattamento per ciò che riguarda la tempestività della diffusione delle notizie.

Art. 9.***(Attività collaterali)***

Il dipendente informa il segretario generale degli eventuali scritti ed articoli che intenda pubblicare nelle materie di competenza del Garante.

Ferme restando le disposizioni di cui agli articoli 58 e 58 bis del d.lg. 3 febbraio 1993, n. 29 e all'art. 1, commi 56 e seguenti, della legge 23 dicembre 1996, n. 662, il dipendente non presta altre attività di lavoro subordinato o autonomo anche di consulenza in materie connesse con quelle di competenza del Garante.

Il dipendente non svolge ulteriori attività esterne che contrastano con i doveri o che incidono sul corretto svolgimento dei compiti d'ufficio.

Il dipendente dichiara al segretario generale le situazioni di cui ai commi 2 e 3 del presente articolo anche al fine delle autorizzazioni e comunicazioni previste dalla legge.

Art. 10.

Il segretario generale informa il collegio delle comunicazioni ricevute e delle autorizzazioni rilasciate ai sensi del presente codice, e sottopone preventivamente all'esame del collegio i casi di cui all'articolo 9, commi 2 e 3.

Art. 11.

Il presidente, i componenti del Garante e il segretario generale conformano la propria attività ai principi del presente codice e si informano reciprocamente degli incontri anche informali cui prendono parte in materie rilevanti per l'attività del Garante.

Art. 12***(Entrata in vigore)***

Il codice entra in vigore il 1 luglio 1998 e può essere aggiornato sulla base dell'esperienza. Le eventuali attività di cui all'articolo 9, comma 2, devono essere cessate entro il 1 ottobre 1998.

Roma, lì 4 giugno 1998

Il Presidente

5.5 PROVVEDIMENTO 29 LUGLIO 1998 – CODICE DI DEONTOLOGIA GIORNALISTICA

PROVVEDIMENTO 29 luglio 1998.

Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica ai sensi dell'art. 25 della legge 31 dicembre 1996, n. 675.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Visto l'art. 25 della legge 31 dicembre 1996, n. 675, come modificato dall'art. 12 del decreto legislativo 13 maggio 1998, n. 171, secondo il quale il trattamento dei dati personali nell'esercizio della professione giornalistica deve essere effettuato sulla base di un apposito codice di deontologia, recante misure ed accorgimenti a garanzia degli interessati rapportati alla natura dei dati, in particolare per quanto riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale;

Visto il comma 4-bis dello stesso art. 25, secondo il quale tale codice è applicabile anche all'attività dei pubblicisti e dei praticanti giornalisti, nonché a chiunque tratti temporaneamente i dati personali al fine di utilizzarli per la pubblicazione occasionale di articoli, di saggi e di altre manifestazioni di pensiero;

Visto il comma 2 del medesimo art. 25, secondo il quale il codice di deontologia è adottato dal Consiglio nazionale dell'Ordine dei giornalisti in cooperazione con il Garante, il quale ne promuove l'adozione e ne cura la pubblicazione nella Gazzetta Ufficiale;

Vista la nota prot. n. 89/GAR del 26 maggio 1997, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad adottare il codice entro il previsto termine di sei mesi dalla data di invio della nota stessa;

Vista la nota prot. n. 4640 del 24 novembre 1997, con la quale il Garante ha aderito alla richiesta di breve differimento del predetto termine di sei mesi, presentata il 19 novembre dal presidente del Consiglio nazionale dell'ordine;

Visto il provvedimento prot. n. 5252 del 18 dicembre 1997, con il quale il Garante ha segnalato al Consiglio nazionale dell'ordine alcuni criteri da tenere presenti nel bilanciamento delle libertà e dei diritti coinvolti dall'attività giornalistica;

Vista la nota prot. n.314 del 23gennaio 1998, con la quale il Garante ha formulato altre osservazioni sul primo schema di codice elaborato dal Consiglio nazionale dell'ordine e trasmesso al Garante con nota prot. n. 7182 del 30 dicembre 1997;

Vista la nota prot. n. 204 del 15 gennaio 1998, con la quale il Garante, sulla base della prima esperienza di applicazione della legge n.675/1996 e dello schema di codice elaborato, ha rappresentato al Ministro di grazia e giustizia l'opportunità di una revisione dell'art. 25 della legge, che è stato poi modificato con il citato decreto legislativo n. 171 del 13 maggio 1998;

Vista la nota prot. n. 5876 del 30 giugno 1998, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad apportare alcune residuali modifiche all'ulteriore schema approvato dallo stesso Consiglio nella seduta del 26 e 27 marzo 1998 e trasmesso al Garante con nota prot. n. 1074 dell'8 aprile;

Constatata l'idoneità delle misure e degli accorgimenti a garanzia degli interessati previsti dallo schema definitivo del codice di deontologia trasmesso al Garante dal Consiglio nazionale dell'ordine con nota prot. n. 2210 del 15 luglio 1998;

Considerato che, ai sensi dell'art. 25, comma 2, della legge n. 675/1996, il codice deve essere pubblicato nella Gazzetta Ufficiale, a cura del Garante, e diviene efficace quindici giorni dopo la sua pubblicazione;

DISPONE

La trasmissione del codice di deontologia che figura in allegato all'ufficio pubblicazione leggi e decreti del Ministero di grazia e giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 29 luglio 1998

Il Presidente: RODOTÀ

ALLEGATO

ORDINE DEI GIORNALISTI
CONSIGLIO NAZIONALE

CODICE DEONTOLOGICO RELATIVO AL TRATTAMENTO DEI DATI PERSONALI
NEL L'ESERCIZIO DELL'ATTIVITÀ GIORNALISTICA AI SENSI DELL'ART. 25
DELLA LEGGE 31 DICEMBRE 1996, N. 675.

Art. 1.
(Principi generali)

1. Le presenti norme sono volte a contemperare i diritti fondamentali della persona con il diritto dei cittadini all'informazione e con la libertà di stampa.

2. In forza dell'art. 21 della Costituzione, la professione giornalistica si svolge senza autorizzazioni o censure. In quanto condizione essenziale per l'esercizio del diritto-dovere di cronaca, la raccolta, la registrazione, la conservazione e la diffusione di notizie su eventi e vicende relativi a persone, organismi collettivi, istituzioni, costumi, ricerche scientifiche e movimenti di pensiero, attuate nell'ambito dell'attività giornalistica e per gli scopi propri di tale attività, si differenziano nettamente per la loro natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti. Su questi principi trovano fondamento le necessarie deroghe previste dai paragrafi 17 e 37 e dall'art. 9 della direttiva 95/46/CE del Parlamento europeo e del Consiglio dell'Unione europea del 24 ottobre 1995 e dalla legge n. 675/1996.

Art. 2.***(Banche dati di uso redazionale e tutela degli archivi personali dei giornalisti)***

1. Il giornalista che raccoglie notizie per una delle operazioni di cui all'art. 1, comma 2, lettera b), della legge n. 675/1996 rende note la propria identità, la propria professione e le finalità della raccolta, salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite. Fatta palese tale attività, il giornalista non è tenuto a fornire gli altri elementi dell'informativa di cui all'art. 10, comma 1, della legge n. 675/1996.

2. Se i dati personali sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a rendere noti al pubblico, mediante annunci, almeno due volte l'anno, l'esistenza dell'archivio e il luogo dove è possibile esercitare i diritti previsti dalla legge n. 675/1996. Le imprese editoriali indicano altresì fra i dati della gerenza il responsabile del trattamento al quale le persone interessate possono rivolgersi per esercitare i diritti previsti dalla legge n. 675/1996.

3. Gli archivi personali dei giornalisti, comunque funzionali all'esercizio della professione e per l'esclusivo perseguimento delle relative finalità, sono tutelati, per quanto concerne le fonti delle notizie, ai sensi dell'art. 2 della legge n. 69/1963 e dell'art. 13, comma 5, della legge n. 675/1996.

4. Il giornalista può conservare i dati raccolti per tutto il tempo necessario al perseguimento delle finalità proprie della sua professione.

Art. 3.***(Tutela del domicilio)***

La tutela del domicilio e degli altri luoghi di privata dimora si estende ai luoghi di cura, detenzione o riabilitazione, nel rispetto delle norme di legge e dell'uso corretto di tecniche invasive.

Art. 4.***(Rettifica)***

Il giornalista corregge senza ritardo errori e inesattezze, anche in conformità al dovere di rettifica nei casi e nei modi stabiliti dalla legge.

Art. 5.***(Diritto all'informazione e dati personali)***

1. Nel raccogliere dati personali atti a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati atti a rivelare le condizioni di salute e la sfera sessuale, il giornalista garantisce il diritto all'informazione su fatti di interesse pubblico, nel rispetto dell'essenzialità dell'informazione, evitando riferimenti a congiunti o ad altri soggetti non interessati ai fatti.

2. In relazione a dati riguardanti circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico, è fatto salvo il diritto di addurre successivamente motivi legittimi meritevoli di tutela.

Art. 6.

(Essenzialità dell'informazione)

1. La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

2. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica.

3. Commenti e opinioni del giornalista appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti.

Art. 7.

(Tutela del minore)

1. Al fine di tutelarne la personalità, il giornalista non pubblica i nomi dei minori coinvolti in fatti di cronaca, né fornisce particolari in grado di condurre alla loro identificazione.

2. La tutela della personalità del minore si estende, tenuto conto della qualità della notizia e delle sue componenti, ai fatti che non siano specificamente reati.

3. Il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca; qualora, tuttavia, per motivi di rilevante interesse pubblico e fermo restando i limiti di legge, il giornalista decida di diffondere notizie o immagini riguardanti minori, dovrà farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi e i limiti stabiliti dalla «Carta di Treviso».

Art. 8.

(Tutela della dignità delle persone)

1. Salva l'essenzialità dell'informazione, il giornalista non fornisce notizie o pubblica immagini o fotografie di soggetti coinvolti in fatti di cronaca lesive della dignità della persona, né si sofferma su dettagli di violenza, a meno che ravvisi la rilevanza sociale della notizia o dell'immagine.

2. Salvo rilevanti motivi di interesse pubblico o comprovati fini di giustizia di polizia, il giornalista non riprende né produce immagini e foto di persone in stato di detenzione senza il consenso dell'interessato.

3. Le persone non possono essere presentate con ferri o manette ai polsi, salvo che ciò sia necessario per segnalare abusi.

Art. 9.*(Tutela del diritto alla non discriminazione)*

1. Nell'esercitare il diritto-dovere di cronaca, il giornalista è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali.

Art. 10.*(Tutela della dignità delle persone malate)*

1. Il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e sempre nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 11.*(Tutela della sfera sessuale della persona)*

1. Il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 12.*(Tutela del diritto di cronaca nei procedimenti penali)*

1. Al trattamento dei dati relativi a procedimenti penali non si applica il limite previsto dall'art. 24 della legge n. 675/1996.

1. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale è ammesso nell'esercizio del diritto di cronaca, secondo i principi di cui all'art. 5.

Art. 13.*(Ambito di applicazione, sanzioni disciplinari)*

1. Le presenti norme si applicano ai giornalisti professionisti, pubblicisti e praticanti e a chiunque altro, anche occasionalmente, eserciti attività pubblicistica.

2. Le sanzioni disciplinari, di cui al titolo III della legge n. 69/1963, si applicano solo ai soggetti iscritti all'albo dei giornalisti, negli elenchi o nel registro.

Il Presidente: PETRINA

5.6 AUTORIZZAZIONI GENERALI AL TRATTAMENTO DEI DATI SENSIBILI

5.6.1 Autorizzazione n. 1/1998 al trattamento dei dati sensibili nei rapporti di lavoro

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la l. 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'art. 22, comma 1, della citata l. n. 675/1996, il quale individua come «sensibili» i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di un'apposita disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità; rilevato altresì che, in base ad una disposizione transitoria (art. 41, comma 5, della citata l. n. 675/1996, come modificato dal d.lg. 8 maggio 1998, n. 135), i soggetti pubblici possono continuare a trattare i dati «sensibili» previa comunicazione al Garante;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati, e che occorre quindi riferire solo a tali soggetti l'ambito di applicazione delle autorizzazioni, fatta eccezione per il trattamento dei dati idonei a rivelare lo stato di salute da parte degli organismi sanitari pubblici, destinatari di autonomo provvedimento in applicazione dell'art. 23 della l. n. 675/1996;

Considerato che il Garante può rilasciare le autorizzazioni, anche d'ufficio, nei confronti di singoli titolari o, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (art. 41, comma 7, l. n. 675/1996, come sostituito dall'art. 4, comma 1, del d.lg. 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 19 novembre 1997 relativa al trattamento dei dati «sensibili» nei rapporti di lavoro, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 21 novembre 1997 e avente efficacia fino al 30 settembre 1998;

Rilevato che è all'esame del Parlamento il disegno di legge governativo che prevede il differimento al 31 luglio 1999 del termine per l'esercizio della delega prevista dalla l. n. 676/1996 e che, entro tale data, dovrebbero essere emanati alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Ritenuto opportuno rilasciare nuove autorizzazioni generali e ciò al fine di proseguire l'intento di semplificazione degli adempimenti che la l. n. 675/1996 pone a carico di determinate categorie di titolari, nonché di assicurare una migliore funzionalità dell'Ufficio del Garante e di armonizzare le prescrizioni da impartire con le autorizzazioni;

Considerata, quindi, l'opportunità che anche le nuove autorizzazioni generali non rechino disposizioni particolarmente dettagliate in una fase tuttora transitoria stante la prevista adozione di norme integrative e correttive in materia, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali in un breve periodo di tempo;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie, in conformità anche a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che le nuove autorizzazioni prendano anch'esse in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla l. n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (art. 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un ampio numero di trattamenti di dati sensibili è effettuato ai fini dell'adempimento di obblighi contabili, retributivi, previdenziali, assistenziali, fiscali e assicurativi nell'ambito dei rapporti di lavoro, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'art. 41, comma 7, della l. n. 675/1996;

AUTORIZZA

il trattamento dei dati sensibili di cui all'art. 22, comma 1, della l. n. 675/1996, finalizzato alla gestione dei rapporti di lavoro, alle condizioni di seguito indicate.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta di parte:

a) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e agli organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee ai sensi della l. 24 giugno 1997, n. 196, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lett. b) e c);

b) a organismi paritetici e ad altri organismi che gestiscono osservatori in materia di lavoro, previsti da leggi, da regolamenti o da contratti collettivi anche aziendali, ovvero dalla normativa comunitaria.

L'autorizzazione riguarda anche l'attività svolta dal medico competente in materia di igiene e di sicurezza del lavoro, in qualità di libero professionista o di dipendente dei soggetti di cui alla lettera a) o di strutture convenzionate.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) a lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione e lavoro, ovvero ad associati anche in compartecipazione e, se necessario in base ai punti 3) e 4), ai relativi familiari e conviventi;

b) a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatarî;

c) a soggetti che effettuano prestazioni coordinate e continuative o ad altri lavoratori autonomi in rapporto di collaborazione con i soggetti di cui al punto 1);

d) a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;

e) a persone fisiche che ricoprono cariche sociali nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);

f) a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

3) Finalità del trattamento

Il trattamento dei dati sensibili deve essere necessario:

a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, da regolamenti o da contratti collettivi anche aziendali, ovvero dalla normativa comunitaria, in particolare ai fini del rispetto della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, di tutela della salute, dell'ordine e della sicurezza pubblica;

b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;

c) per il perseguimento delle finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;

d) per far valere o difendere un diritto in sede giudiziaria, anche da parte di un terzo, sempre che, qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere sia di rango pari a quello dell'interessato.

e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale.

4) Categorie di dati

Il trattamento può avere per oggetto i dati strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), e in particolare:

a) nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;

b) nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati concernenti l'esercizio di funzioni pubbliche e di incarichi politici (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche iniziative, nonché i dati inerenti alle attività o agli incarichi sindacali, ovvero alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;

c) nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti in riferimento a malattie anche professionali, invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni o all'appartenenza a categorie protette.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli artt. 9, 15 e 17 della l. n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza e i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti o alle finalità di cui al punto 3).

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli artt. 10 e 22 della l. n. 675/1996.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. e) della l. n. 675/1996, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 3), ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante verifiche periodiche, deve essere verificata costantemente la stretta pertinenza e la non eccedenza dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e, ove necessario diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, agenzie di intermediazione, associazioni di datori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

Ai sensi dell'art. 23, comma 4, della l. n. 675/1996, i dati idonei a rivelare lo stato di salute possono essere diffusi, solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati idonei a rivelare la vita sessuale non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute:

a) nell'art. 8 della l. 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

b) nell'art. 6 della l. 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;

c) nelle norme in materia di pari opportunità o volte a prevenire discriminazioni.

10) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre 1998, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.6.2 Autorizzazione n. 2/1998 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la l. 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'art. 22, comma 1, della medesima legge, il quale individua come «sensibili» i dati personali idonei a rivelare, tra l'altro, lo stato di salute e la vita sessuale;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità (articolo 22, comma 3, l. n. 675/1996);

Constatato che i soggetti pubblici possono avvalersi di una disposizione transitoria, in base alla quale i trattamenti di dati sensibili iniziati prima dell'8 maggio 1997 possono essere proseguiti fino all'8 novembre 1998 anche in mancanza di una disposizione di legge avente le caratteristiche predette, purché si effettui una comunicazione a questa Autorità (articolo 41, comma 5, l. n. 675/1996, come modificato dal decreto legislativo 8 maggio 1998, n. 135);

Rilevato che gli organismi sanitari pubblici possono avvalersi di tale disposizione transitoria, oppure, a loro scelta, di una disposizione speciale che permette di trattare i dati inerenti alla salute (fatta eccezione, quindi, degli altri dati sensibili) anche in mancanza di una puntuale disposizione di legge e del consenso scritto dell'interessato, qualora perseguano finalità di tutela dell'incolumità fisica e della salute di un terzo o della collettività ed osservino le prescrizioni dell'autorizzazione rilasciata da questa Autorità (articolo 23 l. n. 675/1996);

Considerato che la l. n. 675/1996 prevede che gli esercenti le professioni sanitarie possono trattare: a) i dati idonei a rivelare lo stato di salute, anche senza l'autorizzazione di questa Autorità, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute degli interessati che abbiano manifestato il proprio consenso per iscritto; b) i dati idonei a rivelare lo stato di salute, sulla base di un'autorizzazione, qualora il consenso scritto non sia o non possa essere prestato e i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute di un terzo o della collettività; c) i dati idonei a rivelare la vita sessuale, sulla base del consenso scritto e dell'autorizzazione;

Considerato che gli enti pubblici economici ed ogni altro soggetto privato, inclusi gli organismi sanitari, possono trattare i dati idonei a rivelare lo stato di salute e la vita sessuale solo sulla base del consenso scritto e dell'autorizzazione;

Considerato che il Garante può rilasciare l'autorizzazione anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della l. n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 27 novembre 1997 relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 29 novembre 1997 e avente efficacia fino al 30 settembre 1998;

Rilevato che è all'esame del Parlamento il disegno di legge governativo che prevede il differimento al 31 luglio 1999 del termine per l'esercizio della delega prevista dalla l. n. 676/1996 e che, entro tale data, dovrebbero essere emanati alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, anche in attuazione della raccomandazione N.R (97) 5 adottata dal Consiglio d'Europa in materia di dati sanitari;

Constatato che tali decreti dovranno tener conto del principio affermato nella citata raccomandazione, secondo il quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza di efficacia pari a quelle previste in tale ambito;

Ritenuto opportuno rilasciare una nuova autorizzazione generale volta a proseguire l'intento di semplificazione degli adempimenti previsti dalla l. n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Considerata l'opportunità che anche le nuove autorizzazioni generali non rechino disposizioni particolarmente dettagliate in una fase tuttora transitoria stante la prevista adozione di norme integrative e correttive in materia, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare una nuova autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che anche la nuova autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla l. n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base della citata raccomandazione del Consiglio d'Europa;

Considerato che un numero elevato di trattamenti di dati idonei a rivelare lo stato di salute è effettuato per finalità di prevenzione e di cura, o che riguardano, in particolare, la gestione di servizi socio-sanitari, la ricerca scientifica e la fornitura di prestazioni, beni o servizi all'interessato, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della l. n. 675/1996;

AUTORIZZA:

a) gli esercenti le professioni sanitarie a trattare i dati idonei a rivelare lo stato di salute, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute di un terzo o della collettività, e l'interessato non

abbia prestato il proprio consenso per iscritto o non possa prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere;

b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, con il consenso scritto dell'interessato;

c) gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute qualora ricorrano contemporaneamente le seguenti condizioni:

1) il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;

2) manchi il consenso scritto (articolo 23, comma 1, ultimo periodo, l. n. 675/1996), in quanto l'interessato non lo ha prestato o non può prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere;

3) il trattamento non sia previsto da una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

1) Ambito di applicazione e finalità del trattamento

1.1. L'autorizzazione è rilasciata, anche senza richiesta:

a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;

b) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;

c) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il Servizio sanitario nazionale.

In tali casi, l'autorizzazione è rilasciata al fine di consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, da regolamenti o dalla normativa comunitaria, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di cura e di diagnosi, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffusive, di tutela della salute mentale, di assistenza farmaceutica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini suindicati.

Qualora il perseguimento di tali fini richieda l'espletamento di compiti di organizzazione o di gestione amministrativa, i destinatari della presente autorizzazione devono esigere che i responsabili e gli incaricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione.

1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti:

a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle re-

lazioni tra i fattori di rischio e la salute umana, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. In tali casi occorre acquisire il consenso (fermo restando quanto previsto dall'articolo 23, comma 1, ultimo periodo, della l. n. 675/1996), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima;

b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

c) alle comunità di recupero e di accoglienza, alle case di cura e di riposo, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

d) agli enti, alle associazioni e alle organizzazioni religiose riconosciute, ivi comprese le confessioni religiose e le comunità religiose, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, ove esistenti, nelle rispettive norme statutarie;

e) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi. Se il rapporto intercorre con istituti di credito, imprese assicurative o riguarda valori mobiliari, devono considerarsi indispensabili i soli dati ed operazioni necessari per fornire specifici prodotti o servizi richiesti dall'interessato. Il rapporto può riguardare anche la fornitura di strumenti di ausilio per la vista, per l'udito o per la deambulazione.

f) alle persone fisiche e giuridiche, agli enti, alle associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati e alle operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche.

1.3. La presente autorizzazione è rilasciata, altresì, per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, quando il trattamento sia necessario:

a) ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni;

b) per far valere o difendere un diritto in sede giudiziaria, anche da parte di un terzo, sempre che il diritto sia di rango pari a quello dell'interessato, e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario per il loro perseguimento.

2) Categorie di dati oggetto di trattamento

Il trattamento può avere per oggetto i dati strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 1), e può comprendere le informazioni relative a stati di salute pregressi.

Devono essere considerati sottoposti all'ambito di applicazione della presente autorizzazione, anche i seguenti dati:

a) le informazioni relative ai nati, che devono essere trattate alla stregua dei dati personali in conformità a quanto previsto dalla citata raccomandazione N.R (97) 5 del Consiglio d'Europa;

b) i dati genetici, limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività, sulla base del consenso scritto ai sensi degli articoli 22 e 23 della l. n. 675/1996. In mancanza del consenso, se il trattamento è volto a tutelare l'incolumità fisica e la salute di un terzo o della collettività, il trattamento può

essere iniziato o proseguito solo previa apposita autorizzazione del Garante. I dati genetici non possono essere trattati dai soggetti di cui al punto 1.2, lettere c), d), e) ed f). Le informative all'interessato previste dall'art. 10 della l. n. 675/1996 devono porre in particolare evidenza il diritto dell'interessato di opporsi, per motivi legittimi, al trattamento dei dati genetici che lo riguardano. Fino alla data di entrata in vigore del decreto delegato che darà attuazione alla citata autorizzazione in applicazione della l. 31 dicembre 1996, n. 676, i dati genetici trattati per fini di prevenzione, di diagnosi o di terapia nei confronti dell'interessato, ovvero per finalità di ricerca scientifica, possono essere utilizzati unicamente per tali finalità o per consentire all'interessato di prendere una decisione libera e informata, ovvero per finalità probatorie in sede civile o penale, in conformità alla legge.

3) Modalità di trattamento

Fermi restando gli obblighi previsti dagli artt. 9, 15, 17 e 28 della l. n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, e il trasferimento all'estero dei dati, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato unicamente con logiche e forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti e alle finalità di cui al punto 1).

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli articoli 10, 22 e 23 della l. n. 675/1996. Se l'interessato è minore di età, il consenso può essere prestato disgiuntamente da coloro che esercitano la potestà. Per le informazioni relative ai nati, il consenso è prestato dalla gestante.

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'articolo 9, comma 1, lett. e) della l. 31 dicembre 1996, n. 675, i dati idonei a rivelare lo stato di salute e la vita sessuale possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 1), ovvero per perseguire le finalità ivi menzionate, verificando anche periodicamente la stretta pertinenza e la non eccedenza dei dati trattati.

5) Comunicazione e diffusione dei dati

Ai sensi dell'articolo 23, comma 4, della l. n. 675/1996, i dati idonei a rivelare lo stato di salute possono essere diffusi solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati idonei a rivelare la vita sessuale non possono essere diffusi, salvo il caso in cui la diffusione riguardi dati resi manifestamente pubblici dall'interessato e per i quali l'interessato stesso non abbia manifestato successivamente la sua opposizione per motivi legittimi.

I dati idonei a rivelare lo stato di salute, esclusi i dati genetici, possono essere comunicati, nei limiti strettamente pertinenti agli obblighi, ai compiti e alle finalità di cui al punto 1), a soggetti pubblici e privati, ivi compresi i fondi e le casse di assistenza sanitaria integrativa, le aziende che svolgono attività strettamente correlate all'esercizio di professioni sanitarie o alla fornitura all'interessato di beni, di prestazioni o di servizi, gli istituti di credito e le imprese assicurative, le associazioni od organizzazioni di volontariato e i familiari dell'interessato.

6) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione, relative, ad esempio, al caso in cui la raccolta del consenso comporti un impiego di mezzi manifestamente sproporzionato in ragione, in particolare, del numero di persone interessate.

7) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dall'articolo 5, comma 2, della l. 5 giugno 1990, n.135, il quale prevede che la rilevazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;

b) dall'articolo 11 della l. 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare al medico provinciale competente per territorio una dichiarazione che non faccia menzione dell'identità della donna;

c) dall'articolo 734-bis del c.p., il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato il 25 giugno 1995 dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati e di includerli, in particolare, nelle pubblicazioni a contenuto scientifico o finalizzate all'educazione, alla prevenzione o all'informazione di carattere sanitario.

8) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.6.3 Autorizzazione n. 3/1998 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come «sensibili» i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità (articolo 22, comma 3, legge n. 675/1996);

Constatato che i soggetti pubblici possono avvalersi di una disposizione transitoria, in base alla quale i trattamenti di dati sensibili iniziati prima dell'8 maggio 1997 possono essere proseguiti fino all'8 novembre 1998 anche in mancanza di una disposizione di legge avente le caratteristiche predette, purché si effettui una comunicazione a questa Autorità (articolo 41, comma 5, legge n. 675/1996, come modificato dal decreto legislativo 8 maggio 1998, n. 135);

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati, e che occorre quindi riferire solo a tali soggetti l'ambito di applicazione delle autorizzazioni, fatta eccezione per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, che forma oggetto dell'autorizzazione n. 2/1997;

Considerato che il Garante può rilasciare le autorizzazioni anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 28 novembre 1997 relativa al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 29 novembre 1997 e avente efficacia fino al 30 settembre 1998;

Rilevato che è all'esame del Parlamento il disegno di legge governativo che prevede il differimento al 31 luglio 1999 del termine per l'esercizio della delega prevista dalla legge n. 676/1996 e che, entro tale data, dovrebbero essere emanati alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Ritenuto opportuno rilasciare una nuova autorizzazione generale volta a proseguire l'intento di semplificazione degli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Considerata l'opportunità che anche le nuove autorizzazioni generali non rechino disposizioni particolarmente dettagliate in una fase tuttora transitoria stante la prevista adozione di norme integrative e correttive in materia, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare una nuova autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che anche la nuova autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di questi aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un numero elevato di trattamenti di dati sensibili è effettuato da enti ed organizzazioni di tipo associativo e da fondazioni, per la realizzazione di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo, ove esistenti, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7 della legge n. 675/1996;

AUTORIZZA

il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996 da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) alle associazioni anche non riconosciute, ivi comprese le confessioni religiose e le comunità religiose, i partiti e i movimenti politici, le associazioni e le organizzazioni sindacali, i patronati, le associazioni di categoria, le organizzazioni assistenziali o di volontariato, nonché le federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all'atto costitutivo o ad un contratto collettivo;

b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);

c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.

L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297.

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto in sede giudiziaria, anche da parte di terzi, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato, e i dati siano trattati esclusivamente per tale finalità e per il periodo strettamente necessario per il suo perseguimento.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi e persone giuridiche. I soggetti di cui alle lettere a), b) e c), possono comunicare alle persone giuridiche e agli organismi con scopo di lucro, titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo e le particolari misure di sicurezza adottate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare evidenza, e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto nei punti 3) e 5) in tema di pertinenza e di non eccedenza dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;

b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;

c) ai soggetti che ricoprono cariche sociali o onorifiche;

d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto costitutivo, ove esistenti;

e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;

f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

3) Categorie di dati oggetto di trattamento

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/1997, pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana 29 novembre 1997, n. 279.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 22, comma 1, della legge 31 dicembre 1996, n. 675, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dai regolamenti, dai contratti collettivi o dalla normativa comunitaria.

A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza e la non eccedenza dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni.

4) Modalità di trattamento

Fermi restando gli obblighi previsti dagli artt. 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate alle finalità, agli scopi e agli obblighi di cui al punto 1).

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli articoli 10 e 22 della legge n. 675/1996.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. e) della legge 31 dicembre 1996, n. 675, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità e gli scopi di cui al punto 1), ovvero per adempiere agli obblighi ivi menzionati.

Le verifiche di cui al punto 3) devono riguardare anche la pertinenza e la non eccedenza dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e l'associazione, la fondazione, il comitato o il

diverso organismo, tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto all'associazione, alla fondazione, al comitato o al diverso organismo.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto 1) e tenendo presenti le altre prescrizioni sopraindicate.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti in materia di trattamento di dati personali.

Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio.

9) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre 1998, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.6.4 Autorizzazione n. 4/1998 al trattamento dei dati sensibili da parte dei liberi professionisti

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come «sensibili» i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (articolo 22, comma 1, legge n. 675/1996);

Considerato che i dati idonei a rivelare lo stato di salute e la vita sessuale possono essere trattati anche ai sensi di una speciale disposizione, in base alla quale, ferma restando l'autorizzazione di questa Autorità, si può prescindere dal consenso degli interessati quando il trattamento è necessario per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato, ovvero è necessario per lo svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione del codice di procedura penale, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (articolo 22, comma 4, della citata legge n. 675/1996);

Considerato che il Garante può rilasciare tali autorizzazioni anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 29 novembre 1997 relativa al trattamento dei dati sensibili da parte dei liberi professionisti, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 2 dicembre 1997 e avente efficacia fino al 30 settembre 1998;

Rilevato che è all'esame del Parlamento il disegno di legge governativo che prevede il differimento al 31 luglio 1999 del termine per l'esercizio della delega prevista dalla legge n. 676/1996 e che, entro tale data, dovrebbero essere emanati alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Ritenuto opportuno rilasciare una nuova autorizzazione generale al fine di proseguire l'intento di semplificazione degli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Considerata l'opportunità che anche le nuove autorizzazioni generali non rechino disposizioni particolarmente dettagliate in una fase tuttora transitoria stante la prevista adozione di norme integrative e correttive in materia, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo di tempo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare una nuova autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che anche la nuova autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un numero elevato di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali, e che è pertanto necessario che tali trattamenti formino oggetto di una autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, secondo le prescrizioni di seguito indicate.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta, ai liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, o in conformità alle norme di attuazione dell'articolo 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza.

Sono equiparati ai liberi professionisti i soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'articolo 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'articolo 2232 del codice civile, ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

a) dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/1998;

b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopraindicati, alla quale si riferisce l'autorizzazione generale n. 1/1998;

c) da soggetti privati che svolgono attività investigative, dai giornalisti, dai pubblicisti e dai praticanti giornalisti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69.

2) Interessati ai quali i dati si riferiscono e categorie di dati

Il trattamento può riguardare i dati sensibili relativi ai clienti.

I dati sensibili relativi ai terzi possono essere trattati ove ciò sia strettamente indispensabile per l'esecuzione di specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

In ogni caso, i dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto della citata autorizzazione generale n. 2/1998.

3) Finalità del trattamento

Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;

b) per far valere o difendere un diritto in sede giudiziaria, anche da parte di terzi;

c) ai fini dello svolgimento da parte del difensore nel procedimento penale delle investigazioni di cui all'articolo 38 delle norme di attuazione del codice di procedura penale, anche a mezzo di sostituti e di consulenti tecnici.

4) Modalità di trattamento

Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati.

Restano inoltre fermi gli obblighi:

a) di informare l'interessato ai sensi dell'articolo 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi;

b) di acquisire il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto 3), lettere *b*) e *c*), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari anche in riferimento ai dati idonei a rivelare lo stato di salute o la vita sessuale, solo se i dati sono trattati per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità, oppure per altre finalità con esse non incompatibili.

Le informative devono permettere all'interessato di comprendere agevolmente se il titolare del trattamento è un singolo professionista o un'associazione di professionisti, ovvero se ricorre un'ipotesi di contitolarità tra più liberi professionisti.

Resta ferma la facoltà del libero professionista di designare quali responsabili o incaricati del trattamento i sostituti, gli ausiliari, i tirocinanti e i praticanti presso il libero professionista, i quali, in tal caso, possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Analoga cautela deve essere adottata in riferimento agli incaricati del trattamento preposti all'espletamento di compiti amministrativi.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'articolo 9, comma 1, lettera *e*) della legge n. 675/1996, i dati sensibili possono essere conservati per il periodo di tempo previsto da leggi, regolamenti o dalla normativa comunitaria e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza e la non eccedenza dei dati rispetto agli incarichi.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti e non eccedenti rispetto a successivi incarichi.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale.

I dati idonei a rivelare lo stato di salute possono essere diffusi solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia (articolo 23, comma 4, della legge n. 675/1996).

I dati relativi alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare dalle leggi 20 maggio 1970, n. 300 e 5 giugno 1990, n. 135, nonché dalle norme volte a prevenire discriminazioni.

Restano fermi, altresì, gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

9) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre 1998, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.6.5 Autorizzazione n. 5/1998 al trattamento dei dati sensibili da parte di diverse categorie di titolari

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come «sensibili» i dati personali idonei a rivelare, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (art. 22, comma 1, legge n. 675/1996);

Considerato che il Garante può rilasciare l'autorizzazione anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, nei riguardi di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 15 dicembre 1997 relativa al trattamento dei dati sensibili da parte di diverse categorie di titolari, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 18 dicembre 1997 e avente efficacia fino al 30 settembre 1998;

Rilevato che è all'esame del Parlamento il disegno di legge governativo che prevede il differimento del termine per l'esercizio della delega prevista dalla legge n. 676/1996 al 31 luglio 1999 e che, entro tale data, dovrebbero essere emanati alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Ritenuto opportuno rilasciare una nuova autorizzazione generale al fine di proseguire l'intento di semplificazione degli adempimenti previsti dalla legge n. 675/1996, di armonizzare le prescrizioni da impartire e di favorire la funzionalità dell'Ufficio del Garante;

Considerata l'opportunità che anche le nuove autorizzazioni generali non rechino disposizioni particolarmente dettagliate in una fase tuttora transitoria stante la prevista adozione di norme integrative e correttive in materia, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare una nuova autorizzazione provvisoria, anche in conformità anche a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che anche la nuova autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che numerosi trattamenti di dati sensibili sono effettuati da persone fisiche o giuridiche operanti nei rami assicurativo, previdenziale, assistenziale, bancario, finanziario e di intermediazione finanziaria, nel settore turistico e del trasporto di persone, delle ricerche di mercato, dei sondaggi di opinione o della selezione del personale, nonché della mediazione a fini matrimoniali, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

CAPO I

ATTIVITÀ BANCARIE, CREDITIZIE, ASSICURATIVE, DI GESTIONE DI FONDI O DEL SETTORE TURISTICO O DEL TRASPORTO

1) Soggetti ai quali è rilasciata l'autorizzazione

a) imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;

b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;

c) società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;

d) società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;

e) imprese che svolgono autonome attività strettamente connesse e strumentali a quelle indicate nelle precedenti lettere, e relative alla rilevazione dei rischi, al recupero dei crediti, a lavorazioni massive di documenti, alla trasmissione dati, all'imbustamento o allo smistamento della corrispondenza, nonché alla gestione di esattorie o tesorerie;

f) imprese che operano nel settore turistico o alberghiero o del trasporto, le agenzie di viaggio e gli operatori turistici.

2) Finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale, dalla legge, dai regolamenti, dalla normativa comunitaria o dai contratti collettivi, o prescritti da autorità od organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'articolo 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (articolo 13, comma 1, lettera c), n. 4) legge n. 675/1996), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

I dati sensibili non possono essere diffusi.

CAPO II

SONDAGGI E RICERCHE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

Imprese, società, istituti ed altri organismi o soggetti privati, ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il sondaggio o la ricerca devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato e che abbiano risposto a questionari o ad interviste effettuate nell'ambito di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il consenso deve essere manifestato in ogni caso per iscritto.

I dati personali di natura sensibile possono essere trattati solo se il trattamento di dati anonimi non permette al sondaggio o alla ricerca di raggiungere i suoi scopi.

3) Conservazione dei dati

Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione.

I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la fase contestuale alla registrazione dei campioni raccolti. La registrazione deve essere effettuata senza ritardo anche nel caso in cui i campioni siano stati raccolti in numero elevato.

Entro tale ambito temporale, resta ferma la possibilità per il titolare della raccolta, nonché per i suoi responsabili o incaricati, di utilizzare i dati personali al fine di verificare presso gli interessati la veridicità o l'esattezza dei campioni.

4) Comunicazione dei dati

I dati sensibili non possono essere né comunicati né diffusi.

I campioni del sondaggio o della ricerca possono essere comunicati o diffusi in forma individuale o aggregata, sempre che non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

CAPO III**ATTIVITÀ DI ELABORAZIONE DI DATI****1) Soggetti ai quali è rilasciata l'autorizzazione**

Imprese, società, istituti ed altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di altri soggetti, e che presuppone l'elaborazione di dati ed altre operazioni di trattamento eseguite in materia di lavoro ovvero a fini contabili, retributivi, previdenziali, assistenziali e fiscali.

2) Prescrizioni applicabili

Il trattamento è regolato dalle autorizzazioni:

a) n. 1/1998, emanata il 30 settembre 1998, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;

b) n. 4/1998, emanata il 30 settembre 1998, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

CAPO IV

ATTIVITÀ DI SELEZIONE DEL PERSONALE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di un'attività svolta anche di propria iniziativa nell'interesse di terzi, ai soli fini della ricerca o della selezione di personale.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i candidati forniscano dati di propria iniziativa, in particolare attraverso l'invio di *curricula*.

Non è consentito il trattamento dei dati:

- a) idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni a carattere religioso, filosofico, politico o sindacale, l'origine razziale ed etnica, e la vita sessuale;
- b) inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
- c) in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

3) Comunicazione e diffusione dei dati

I dati idonei a rivelare lo stato di salute possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui ai punti 1) e 2), a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato.

I dati sensibili non possono essere diffusi.

CAPO V

MEDIAZIONE A FINI MATRIMONIALI

1) Soggetti ai quali è rilasciata l'autorizzazione

L'autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati che esercitano, anche attraverso agenzie autorizzate, un'attività di mediazione a fini matrimoniali o di instaurazione di un rapporto di convivenza.

2) Finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, ai soli fini dell'esecuzione dei singoli incarichi conferiti in conformità alle leggi e ai regolamenti.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i soli dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza.

Non è consentito il trattamento di dati relativo a persone minori di età in base all'ordinamento del Paese di appartenenza o, comunque, in base alla legge italiana.

4) Categorie di dati oggetto di trattamenti

Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

5) Comunicazione dei dati

I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (articolo 13, comma 1, lettera c), n. 4), della legge n. 675/1996), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

L'eventuale diffusione anche per via telematica di taluni dati sensibili deve essere oggetto di apposita autorizzazione di questa Autorità.

6) Norme finali

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti, in particolare nell'ambito della legge penale e della disciplina di pubblica sicurezza, nonché in materia di tutela dei minori.

CAPO VI

PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati idonei a rivelare lo stato di salute

Il trattamento dei dati idonei a rivelare lo stato di salute deve essere effettuato anche nel rispetto dell'autorizzazione n. 2/1998, emanata il 30 settembre 1998.

Il trattamento dei dati genetici non è consentito nei casi previsti dalla presente autorizzazione.

2) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza e i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e forme di organizzazione dei dati strettamente correlate alle finalità indicate nei capi che precedono.

Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'articolo 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi.

3) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lettera e) della legge 31 dicembre 1996, n. 675, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi, verificando anche periodicamente la stretta pertinenza e la non eccedenza dei dati trattati.

Restano fermi i diversi termini di conservazione previsti dalle leggi o dai regolamenti.

Resta altresì fermo quanto previsto nel capo II in materia di sondaggi e di ricerche.

4) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

5) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dalla legge 20 maggio 1970, n. 300;

b) dalla legge 5 giugno 1990, n. 135.

Restano altresì fermi gli obblighi deontologici, nonché gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati.

6) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre 1998, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.6.6 Autorizzazione n. 6/1998 al trattamento di alcuni dati sensibili da parte degli investigatori privati

PROVVEDIMENTO 30 settembre 1998

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come «sensibili» i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Considerato che il trattamento di questi dati da parte di privati ed enti pubblici economici è permesso, di regola, solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (articolo 22, comma 1, legge n. 675/1996);

Considerato che una speciale disposizione (articolo 22, comma 4, legge n. 675/1996) permette di trattare i dati idonei a rivelare lo stato di salute e la vita sessuale senza il consenso degli interessati, quando il trattamento autorizzato dal Garante è necessario per svolgere una investigazione nell'ambito di un procedimento penale (articoli 190 del codice di procedura penale e 38 delle relative norme di attuazione) o, comunque, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato;

Vista l'autorizzazione del Garante adottata il 29 dicembre 1997 relativa al trattamento di alcuni dati sensibili da parte degli investigatori privati, pubblicata sulla «Gazzetta Ufficiale» della Repubblica italiana il 2 gennaio 1998 e avente efficacia fino al 30 settembre 1998;

Considerato che il Garante ha rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/1998, emanata il 30 settembre 1998), anche in riferimento alle predette finalità di ordine giudiziario;

Considerato che numerosi trattamenti aventi tali finalità sono effettuati con l'ausilio di investigatori privati, e che è pertanto opportuno integrare le prescrizioni dell'autorizzazione n. 2/1998 mediante un ulteriore provvedimento di ordine generale che tenga conto dello specifico contesto dell'investigazione privata, anche al fine di armonizzare le prescrizioni da impartire alla categoria;

Ritenuta la necessità di applicare anche al caso di specie le considerazioni già espresse con l'autorizzazione n. 2/1998 per ciò che riguarda la natura provvisoria delle autorizzazioni generali e i criteri direttivi prescelti per la determinazione delle relative prescrizioni;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione dell'apposito codice di deontologia e di buona condotta che il Garante è in procinto di promuovere (articolo 22, comma 4, legge n. 675/1996);

AUTORIZZA

gli investigatori privati a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, secondo le prescrizioni di seguito indicate.

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, alle persone fisiche e giuridiche, agli istituti, agli enti, alle associazioni e agli organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (articolo 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento può essere effettuato unicamente:

a) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile;

b) su incarico di un difensore nell'ambito del procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (articoli 190 del codice di procedura penale e 38 delle relative norme di attuazione).

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni nel procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/1998, emanata il 30 settembre 1998);

b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione generale n. 2/1998, emanata il 30 settembre 1998);

c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione generale n. 3/1998, emanata il 30 settembre 1998);

d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione generale n. 4/1998, emanata il 30 settembre 1998).

2) Categorie di dati e interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1).

I dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

3) Modalità di trattamento

Gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati idonei a rivelare lo stato di salute e la vita sessuale. Tali attività possono essere eseguite esclusivamente sulla base di un apposito incarico conferito per iscritto, anche da un difensore, per le esclusive finalità di cui al punto 1).

L'atto di incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole fissato per la sua ultimazione.

I dati devono essere registrati ed elaborati mediante logiche e forme di organizzazione strettamente correlate alle finalità di cui al punto 1).

L'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'articolo 10, comma 1, della legge n. 675/1996, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore nonché la natura facoltativa del conferimento dei dati.

Nel caso in cui i dati sono raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (articoli 10, commi 3 e 4 e 22, comma 4, legge n. 675/1996), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive, oppure se i dati sono utilizzati per ulteriori finalità non incompatibili con quelle precedentemente perseguite.

Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

L'investigatore privato deve eseguire personalmente l'incarico ricevuto, e non può avvalersi di altri investigatori non indicati nominativamente all'atto del conferimento dell'incarico.

Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli articoli 8 e 19 della legge n. 675/1996, l'investigatore privato deve vigilare con cadenza almeno settimanale sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Per quanto non previsto nella presente autorizzazione, il trattamento deve essere effettuato nel rispetto delle ulteriori prescrizioni contenute nella citata autorizzazione generale n. 2/1998, in particolare per ciò che riguarda le informazioni relative ai nascituri e ai dati genetici.

Il trattamento dei dati deve inoltre rispettare le prescrizioni di un apposito codice di deontologia e di buona condotta, che il Garante è in procinto di promuovere ai sensi degli articoli 22, comma 4 e 31, comma 1, lettera h), della legge n. 675/1996.

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'articolo 9, comma 1, lettera e) della legge n. 675/1996, i dati sensibili possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza e la non eccedenza dei dati rispetto alle finalità perseguite e all'incarico conferito.

Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico.

La mera pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

5) Comunicazione e diffusione dei dati

I dati possono essere comunicati unicamente al soggetto che ha conferito l'incarico.

I dati non possono essere comunicati ad un altro investigatore privato, salvo che questi sia stato indicato nominativamente nell'atto di incarico e la comunicazione sia necessaria per lo svolgimento dei compiti affidati.

I dati idonei a rivelare lo stato di salute possono essere diffusi solo se è necessario per finalità di prevenzione, accertamento o repressione dei reati (articolo 23, comma 4, della legge n. 675/1996), con l'osservanza delle norme che regolano la materia.

I dati relativi alla vita sessuale non possono essere diffusi.

6) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

7) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare:

a) dagli articoli 4 (impianti e apparecchiature per finalità di controllo a distanza dei lavoratori) e 8 (indagini sulle opinioni del lavoratore o su altri fatti non rilevanti ai fini della valutazione dell'attitudine professionale) della legge 20 maggio 1970, n. 300;

b) dalla legge 5 giugno 1990, n. 135, in materia di sieropositività e di infezione da HIV;

c) dalle norme processuali o volte a prevenire discriminazioni;

d) dall'articolo 734-bis del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano fermi gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati.

Restano fermi, in particolare, gli obblighi previsti in tema di liceità e di correttezza nell'uso di strumenti o apparecchiature che permettono la raccolta di informazioni anche sonore o visive, ovvero in tema di accesso a banche dati o di cognizione del contenuto della corrispondenza e di comunicazioni o conversazioni telefoniche, telematiche o tra soggetti presenti.

Resta ferma la facoltà per le persone fisiche di trattare direttamente dati per l'esclusivo fine della tutela di un proprio diritto in sede giudiziaria, anche nell'ambito delle investigazioni relative ad un procedimento penale. In tali casi, la legge n. 675/1996 non si applica anche se i dati sono comunicati occasionalmente ad una autorità giudiziaria o a terzi, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 3 legge n. 675/1996).

8) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1 ottobre 1998, fino al 30 settembre 1999.

La presente autorizzazione sarà pubblicata nella «Gazzetta Ufficiale» della Repubblica italiana.

Roma, 30 settembre 1998

Il Presidente

5.7 GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

5.7.1 Documento di lavoro: notifica

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni, diritto delle società e informazioni finanziarie

Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

XV/50271/97 IT
def.
WP 8

Gruppo di lavoro sulla protezione delle persone
per quanto riguarda il trattamento dei dati personali

Documento di lavoro: Notifica

Adottato dal gruppo di lavoro il 3 dicembre 1997

1. INTRODUZIONE

La sezione IX ²⁹⁾ del capitolo II della direttiva 95/46/CE relativa alla tutela delle persone fisiche per quanto riguarda il trattamento dei dati personali nonché la libera circolazione di tali dati («la direttiva») disciplina la notifica del trattamento dei dati alle autorità nazionali di controllo («le autorità»).

Il gruppo di lavoro, sulla base del mandato previsto all'articolo 30, n. 1, lettera a), della direttiva, ha avviato discussioni nel corso della seconda riunione sulla possibile attuazione delle disposizioni della direttiva in materia di notifica. Una serie di documenti di lavoro riguardanti specificamente la semplificazione e l'esenzione dall'obbligo di notificare il trattamento dei dati alle autorità sono stati presentati dalle delegazioni francese, olandese e britannica.

Per quanto riguarda la semplificazione e l'esenzione dall'obbligo di notificare, la delegazione tedesca ha presentato un documento di lavoro sul ruolo, in Germania, del funzionario indipendente incaricato della protezione dei dati (funzionario interno per la protezione dei dati) di cui all'articolo 18, n. 2, della direttiva ³⁰⁾. La discussione su questo tema è continuata durante la terza riunione dopo la presentazione dei rappresentanti dei funzionari responsabili per la protezione dei dati in Germania.

²⁹⁾ In particolare gli articoli da 18 a 20.

³⁰⁾ Documento di lavoro 1 discusso durante la seconda riunione.

Ci si è trovati d'accordo sul fatto che il gruppo di lavoro potesse utilmente fornire alcuni orientamenti sull'interpretazione delle disposizioni della direttiva. L'esperienza di alcune delegazioni nell'applicazione di disposizioni nazionali attualmente in vigore analoghe a quelle della direttiva poteva fornire indicazioni sul funzionamento delle varie opzioni presentate nella direttiva.

La discussione ha mostrato che la specificazione delle finalità al momento della notifica svolge un ruolo importante nell'applicazione del principio dell'indicazione dello scopo³¹⁾. Il ruolo degli «scopi notificati» nell'attuale normativa nazionale varia nei differenti ordinamenti giuridici, così come il livello di dettaglio nella descrizione di tali scopi, non solo tra gli Stati membri ma anche all'interno degli Stati membri.

Il gruppo di lavoro ha concordato di scambiare modelli di moduli di notifica al fine di studiare il tipo di specificazione delle finalità nei vari Stati membri. Tali modelli sono stati distribuiti durante la terza riunione.

Una versione precedente del presente documento è stata discussa nel corso della quarta riunione.

Esempi di descrizione della finalità delle operazioni di trattamento effettuate da una banca, uno studio medico e una compagnia telefonica sono stati scambiati nel corso della quinta riunione ed hanno costituito la base della discussione.

La sezione seguente descrive gli antecedenti legislativi delle disposizioni della direttiva. La sezione terza riassume alcune delle principali caratteristiche dell'attuale situazione normativa a livello nazionale. L'ultima sezione delinea alcune conclusioni preliminari ed esamina alcuni punti relativi al modo in cui il gruppo di lavoro dovrebbe affrontare il tema della notifica.

2. ANTECEDENTI LEGISLATIVI DELLE DISPOSIZIONI DELLA DIRETTIVA IN TEMA DI NOTIFICA

La proposta originale della Commissione³²⁾ conteneva due disposizioni riguardanti la notifica: l'art. 7, riguardante gli archivi del settore pubblico e l'art. 11, riguardante gli archivi del settore privato. Il considerando 13 chiariva l'identica finalità delle due disposizioni: garantire «la trasparenza indispensabile all'esercizio del diritto di accesso di qualsiasi persona ai dati che la riguardano». L'obbligo di notifica riguardava solo «i dati personali che potrebbero essere comunicati».

Una serie di emendamenti del Parlamento hanno modificato sostanzialmente tali disposizioni. La proposta modificata in base agli emendamenti parlamentari ha ristrutturato l'intero sistema di notifica.

La distinzione tra il settore pubblico e il settore privato è stata abolita e le norme sulla modifica sono state riferite a tutte le operazioni di trattamento. La relazione, tuttavia, ha sottolineato che la potenziale estensione dell'obbligo di notifica deve essere considerata in combinazione con l'introduzione di deroghe all'obbligo di notifica e di semplificazione delle procedure.

Anche il fine generale della notifica è stato modificato: esso deve costituire la base del controllo selettivo di legittimità delle operazioni di trattamento da parte delle autorità di controllo.

³¹⁾ A questo principio si fa a volte riferimento come principio di «finalità».

³²⁾ COM(90) 314 def. - SYN 287.

Alcuni aspetti della proposta modificata contribuiscono infatti ad eliminare requisiti burocratici non necessari. Una singola notifica può comprendere l'insieme di procedure di trattamento con identica finalità. Inoltre i responsabili del controllo dei dati non hanno l'obbligo di fornire eccessivi particolari perché la notifica deve indicare unicamente le categorie di soggetti interessati, di soggetti destinatari e di dati. La notifica non è necessaria per il trattamento di dati riguardanti i membri e i contatti degli organismi senza fini di lucro indicati all'art. 8, n. 2, lettera d). Infine, è considerata opzionale la notifica del trattamento non automatico di dati personali.

La proposta modificata non si proponeva unicamente di limitare o semplificare gli obblighi di notifica ma, secondo gli auspici del Parlamento, intendeva creare un sistema a tre livelli che, pur evitando gli eccessi burocratici, fornisse vari gradi di protezione in rapporto ai rischi posti da vari tipi di operazioni di trattamento.

Veniva introdotto un sistema di autorizzazione preventiva riguardante operazioni di trattamento che presentavano «rischi specifici». La relazione faceva riferimento al trattamento di dati sensibili, alle «liste nere» e alle «operazioni volte ad informare i terzi sulla solvibilità delle persone» come esempi di operazioni di trattamento che potevano richiedere un controllo preventivo.

Il testo finale delle disposizioni sulla notifica conservava la struttura generale della proposta modificata. Venivano tuttavia aggiunte semplificazioni e deroghe dall'obbligo di notifica riguardanti i pubblici registri e le situazioni in cui il responsabile del registro designa, in conformità con il diritto nazionale, un funzionario interno addetto alla protezione dei dati. Il considerando 48 chiarisce che il fine delle procedure di notifica è di chiarire gli scopi e le principali caratteristiche delle operazioni di trattamento al fine di verificarne la conformità con la normativa sulla protezione dei dati.

Il considerando 52 indica che il controllo ex-post costituisce la forma normale di controllo da parte delle autorità. I considerando 53 e 54 confermano che il controllo preventivo rappresenta una procedura in qualche modo eccezionale da utilizzare solo in rapporto a specifici rischi.

3. SITUAZIONE ATTUALE NEL DIRITTO NAZIONALE

Procedure di notifica del trattamento dei dati alle autorità esistono attualmente in tutte le normative nazionali relative alla protezione dei dati. Tuttavia l'estensione dell'obbligo di notifica varia notevolmente.

In Spagna, Lussemburgo, Austria, Portogallo, Svezia e Regno Unito in linea generale, tutte le operazioni di trattamento che rientrano nella sfera d'applicazione della legge sulla protezione dei dati³³⁾ devono essere notificate alle autorità responsabili per la protezione dei dati.

³³⁾ In alcuni di questi paesi la normativa sulla protezione dei dati si applica attualmente solo ai dati trattati automaticamente, non disciplinando altri tipi di operazioni di trattamento. Nel Regno Unito, ad esempio, i dati personali elaborati per finalità domestiche o ricreative, le informazioni che per legge devono essere rese pubbliche, i dati elaborati per finalità di sicurezza nazionale, di pagamento di stipendi e salari, di pensioni e di conti correnti, quelli relativi a circoli privi di personalità giuridica e gli elenchi di indirizzi sono esonerati dagli obblighi previsti dalla maggior parte delle disposizioni degli atti normativi sulla protezione dei dati.

Alcuni di questi paesi stanno attualmente semplificando i requisiti di notifica o stanno introducendo deroghe agli obblighi di notificare. I sistemi generali di notifica sono risultati in alcuni casi particolarmente costosi in termini di utilizzazione delle risorse per le autorità responsabili. Inoltre, non è stato sempre facile effettuare controlli significativi sulla base delle notifiche.

In Belgio e nei Paesi Bassi la maggior parte dei normali e meno rischiosi tipi di operazioni di trattamento sono state esentate dall'obbligo di notifica attraverso un atto governativo adottato nell'ambito della normativa generale sulla protezione dei dati. Le deroghe riguardano un'ampia proporzione dei vari tipi di trattamento dei dati (secondo le stime, circa l'80%).

In Francia, le categorie più normali e meno rischiose di trattamento dei dati sono soggette a una procedura semplificata di notifica secondo la quale il responsabile dell'archivio dichiara semplicemente di operare in conformità con una cosiddetta «norme simplifiée» predeterminata dalla Commission Nationale Informatique et Libertés (CNIL). Sono state sino ad oggi definite 40 «normes simplifiées» comprendenti un gran numero di operazioni di trattamento (il 75% delle notifiche per il 1995 sono state notifiche semplificate).

In Italia, numerose deroghe dall'obbligo di notifica sono state introdotte attraverso decreti adottati nel quadro della normativa generale sulla protezione dei dati. Tali deroghe riguardano alcune categorie di operazioni di trattamento e sono soggette a condizioni specifiche.

In Danimarca ³⁴⁾, Germania, Irlanda e Finlandia l'obbligo di notifica comprende solo alcuni tipi di operazioni di trattamento ³⁵⁾. La notifica viene effettuata di solito attraverso speciali moduli cartacei. In Belgio è inoltre possibile notificare su dischetti elettronici ³⁶⁾. Nel Regno Unito la registrazione può essere effettuata in parte per telefono, ma devono in ogni caso essere riempiti i moduli prestampati con ulteriori informazioni. I moduli di notifica possono comprendere di solito tutti i tipi di operazioni di trattamento. Nel Regno Unito, tuttavia, sono stati creati moduli speciali: si tratta di normali moduli di notifica nei quali sono state evidenziate tutte le parti normalmente relative a un certo tipo di gestione di dati.

I moduli di notifica comprendono di solito particolari sui responsabili degli archivi e sulle operazioni di trattamento, quali i tipi di dati trattati, gli scopi delle operazioni di trattamento, le persone che hanno accesso ai dati e così via.

Un elemento fondamentale della notifica è la descrizione dello scopo dell'operazione di trattamento. La prassi relativa all'indicazione degli scopi varia tra gli Stati membri.

In Belgio e nel Regno Unito un elenco predeterminato comprendente i possibili scopi del trattamento è allegato al modulo di notifica. Coloro che gestiscono

³⁴⁾ In Danimarca l'obbligo di notifica comprende tutte le operazioni di trattamento nel settore pubblico, ma solo alcuni tipi di operazioni di trattamento nel settore privato.

³⁵⁾ In Germania gli organismi del settore pubblico federale devono notificare al Commissario federale per la protezione dei dati mentre gli organismi dei Länder notificano ai Commissari dei Länder stessi. Tale procedura non è tuttavia obbligatoria in tutti i Länder. Nel settore privato hanno l'obbligo di notificare solo alcuni operatori del settore del credito, gli operatori nel settore delle vendite dirette e le organizzazioni che trattano dati per conto di altri. In Finlandia deve essere notificato il trattamento dei dati destinati alle vendite dirette, alle ricerche di opinioni o di mercato e alle chiamate di richiesta di numeri di abbonati telefonici.

³⁶⁾ Questo tipo di notifica è particolarmente vantaggioso per i bassi costi.

i dati possono pertanto scegliere uno degli scopi predefiniti ³⁷⁾. In nessuno dei due paesi, tuttavia, coloro che gestiscono i dati sono obbligati a fare riferimento ad uno degli scopi predeterminati; essi possono indicare altri scopi negli spazi previsti.

Le discussioni nel corso della seconda riunione e i modelli di notifica scambiati durante la terza hanno mostrato che i responsabili degli archivi tendono a fornire descrizioni molto brevi e spesso generiche degli scopi delle operazioni di trattamento.

Nella maggior parte degli Stati membri l'analisi a posteriori della compatibilità delle operazioni con la finalità del trattamento, non viene effettuata in rapporto alla descrizione astratta, ma facendo riferimento agli scopi concreti delle varie operazioni.

L'indicazione di finalità generiche al momento della notifica priva quest'ultima della sua funzione. La descrizione generica dello scopo non consente alle autorità responsabili per la protezione dei dati di valutare se una particolare operazione di trattamento è conforme alla legge e ha scarsa utilità per coloro che consultano il registro pubblico delle operazioni di trattamento.

4. CONCLUSIONI

La notifica contribuisce al rispetto dei principi della direttiva poiché i responsabili degli archivi, al fine di effettuare la notifica, devono valutare e descrivere le loro operazioni di trattamento, definendo in anticipo quali dati saranno utilizzati e a quale scopo. Per svolgere in modo adeguato queste funzioni e contribuire alla trasparenza del trattamento dei dati, le informazioni fornite non devono essere generiche ma specifiche.

È particolarmente importante che gli scopi delle operazioni di trattamento siano adeguatamente indicati. Definizioni eccessivamente generiche degli scopi delle operazioni di trattamento rendono inutile l'intero sistema delle notifiche. Né coloro cui i dati si riferiscono né le autorità di controllo saranno in grado di valutare l'operazione notificata o la compatibilità delle varie operazioni pianificate o realizzate dai responsabili degli archivi con lo scopo per il quale i dati sono stati originariamente raccolti o ulteriormente elaborati.

Valutare la compatibilità delle varie operazioni con lo scopo per il quale i dati sono stati originariamente raccolti e che è stato notificato alle autorità responsabili per la protezione dei dati è uno dei compiti più difficili e importanti nella procedura di verifica della conformità con la normativa sulla protezione dei dati. Il gruppo di lavoro intende sviluppare metodi comuni per valutare la compatibilità dello scopo delle operazioni di trattamento.

Forti divergenze nella descrizione dello scopo delle operazioni di trattamento nei vari Stati membri non rappresenterebbero solo un problema per coloro che gestiscono i dati, ma potrebbero vanificare l'equivalenza del livello di protezione nell'ambito comunitario. L'analisi delle attuali misure nazionali di notifica mostra che non vi sono fondamentali differenze nella descrizione degli scopi tra i vari Stati membri. Tuttavia, la tipologia e la quantità dei particolari forniti varia tra le varie procedure nazionali e secondo la struttura dei moduli di notifica.

³⁷⁾ Ve ne sono circa 54 in Belgio e 70 nel Regno Unito.

L'esperienza degli Stati membri nei quali sono applicate tali misure dimostra che gli elenchi predeterminati e gli scopi più comuni sono particolarmente apprezzati dai responsabili degli archivi e semplificano la gestione delle notifiche da parte delle autorità. Il gruppo di lavoro continuerà a studiare la possibilità di definire una descrizione normalizzata degli scopi delle normali operazioni di trattamento che dovrà costituire un orientamento per tutti gli interessati.

Requisiti eccessivamente burocratici relativi alla notifica non rappresentano solamente un onere per le imprese ma sono in contrasto con la ratio stessa della procedura di notifica, costituendo un onere eccessivo per le autorità responsabili della protezione dei dati. Alcuni paesi hanno introdotto o hanno mostrato interesse nelle procedure semplificate di notifica o nelle deroghe all'obbligo di notifica. In base alla direttiva, le notifiche semplificate o le deroghe all'obbligo di notifica possono essere concesse in rapporto alle operazioni di trattamento che hanno scarse probabilità d'influenzare negativamente i diritti e le libertà di coloro cui i dati si riferiscono. Alcuni elementi devono essere specificati in rapporto a tali operazioni di trattamento³⁸⁾.

Le notifiche semplificate o le deroghe possono inoltre essere concesse nei casi in cui i responsabili degli archivi, in conformità con la normativa nazionale, designano un funzionario interno responsabile per la protezione dei dati. Quest'ultimo deve garantire che i diritti e le libertà di coloro cui i dati si riferiscono hanno scarse probabilità di essere influenzati negativamente dalle operazioni di trattamento. A tal fine, secondo la direttiva, il funzionario deve come minimo garantire in modo indipendente l'applicazione delle disposizioni nazionali adottate sulla base della direttiva e mantenere un registro delle operazioni di trattamento comprendente gli elementi d'informazione normalmente presenti nel registro pubblico delle operazioni di trattamento.

La creazione di funzionari interni responsabili della protezione dei dati limita la necessità di un controllo centralizzato. Il gruppo di lavoro appoggia la creazione di tali funzionari su base obbligatoria o volontaria. È tuttavia necessario che siano forniti loro gli strumenti per svolgere le loro funzioni in modo efficace. Se tali poteri e risorse sono insufficienti a garantire i diritti e le libertà di coloro cui i dati si riferiscono, le deroghe dal normale obbligo di notifica non sarebbero più giustificate.

L'effettiva indipendenza di tali funzionari nel garantire l'applicazione della legge sulla protezione dei dati è essenziale per la protezione dei diritti di coloro cui i dati si riferiscono e per verificare la conformità con la normativa in materia. Vi dovranno essere adeguate garanzie che questi funzionari possano agire nello svolgimento delle loro funzioni in piena indipendenza, soprattutto dai dirigenti delle imprese.

Esiste un certo grado di coerenza per quanto riguarda le categorie di operazioni che hanno scarsa probabilità d'influenzare negativamente i diritti e le libertà di coloro cui i dati si riferiscono. Tali categorie comprendono l'elaborazione di dati relativa alla gestione delle buste paga, alla contabilità, ai partner e azionisti, ai clienti e fornitori, ecc.

³⁸⁾ [...] gli scopi del trattamento, i dati o le categorie di dati sottoposti a trattamento, la categoria o le categorie di soggetti cui i dati si riferiscono, i destinatari o le categorie di destinatari dei dati e il periodo di tempo durante il quale i dati sono conservati» (art. 18, n. 2).

Il gruppo di lavoro intende continuare nei suoi sforzi di definire un elenco di operazioni di trattamento che, indipendentemente dalle misure procedurali adottate dagli Stati membri per il recepimento delle relative disposizioni della direttiva, possa essere utilizzato come riferimento per decidere quali operazioni hanno meno probabilità d'influenzare negativamente i diritti e le libertà di coloro cui i dati si riferiscono.

La notifica tramite strumenti diversi dai moduli cartacei rende la notifica stessa più efficace sia per i responsabili degli archivi che per le autorità. Il gruppo di lavoro appoggia l'utilizzazione di tali forme di notifica quali strumenti per ridurre i costi per gli operatori economici e consentire un controllo meno costoso e più efficiente da parte delle autorità.

Una delle funzioni delle procedure di notifica è d'informare il pubblico sulle operazioni di trattamento esistenti tramite il registro pubblico. Il gruppo di lavoro ritiene estremamente importante rendere tale registro facilmente accessibile al pubblico. Il gruppo di lavoro considera con particolare interesse i progetti volti a rendere i registri pubblici disponibili attraverso la world wide web. Sottolinea infine l'esigenza di adottare adeguate garanzie volte ad evitare che i dati personali compresi nei registri delle operazioni di trattamento siano utilizzati in modo improprio.

5.7.2 Utilizzazione di disposizioni contrattuali nel trasferimento di dati personali verso Paesi terzi

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni - Diritto delle società e informazioni finanziarie

Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

DG XV D/5005/98 def.
WP 9

Gruppo di lavoro per la tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Documento di lavoro: Pareri preliminari circa l'utilizzazione di disposizioni contrattuali nel contesto del trasferimento di dati personali verso paesi terzi

approvato dal gruppo di lavoro il 22 aprile 1998

1. INTRODUZIONE

Nel documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997 e intitolato «Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza», il gruppo di lavoro ha promesso di esaminare nei suoi lavori futuri le circostanze nelle quali soluzioni contrattuali *ad hoc* possano costituire mezzi idonei per garantire la tutela delle persone fisiche ove dati personali vengano trasferiti verso un paese terzo in cui il livello di protezione non sia in genere adeguato. Il presente documento mira a fornire una base per tale esame.

In base al principio di cui all'articolo 25, paragrafo 1 della direttiva relativa alla protezione dei dati (95/46/CE), il trasferimento di dati personali verso paesi terzi può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato. All'articolo 26, paragrafo 1, figurano alcune deroghe a tale norma, che non vengono però esaminate nel presente documento. Obiettivo di quest'ultimo è quello di esaminare l'eventuale ulteriore possibilità di deroga al principio della «protezione adeguata» dell'articolo 25 come stabilito all'articolo 26, paragrafo 2. Tale disposizione permette a uno Stato membro di autorizzare un trasferimento o una categoria di trasferimenti verso un paese terzo «non adeguato» «qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi». La disposizione in seguito specifica che «tali garanzie possono segnatamente risultare da clausole contrattuali». Ai sensi dell'articolo 26, paragrafo 4, inoltre la Commissione può, secondo la procedura di cui all'articolo 31, decidere che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui all'articolo 26, paragrafo 2.

L'idea di avvalersi di contratti come mezzo per regolamentare i trasferimenti internazionali di dati personali non è stata ovviamente inventata dalla direttiva. Già nel 1992 il Consiglio d'Europa, la Camera di commercio internazionale e la Commissione europea avevano svolto insieme uno studio in merito³⁹⁾. In tempi più recenti un numero sempre crescente di esperti e di commentatori, forse notando l'esplicito riferimento nella direttiva, hanno formulato in studi e articoli osservazioni circa l'utilizzazione di contratti. Questi ultimi hanno continuato ad essere utilizzati nel «mondo reale» come mezzo per ovviare ai problemi inerenti alla protezione dei dati derivanti dal trasferimento di dati personali da alcuni Stati membri Ue. I contratti sono stati largamente utilizzati in Francia a partire dalla fine degli anni '80, mentre in Germania il recente caso della «Bahncard» che ha coinvolto la Citibank è stato oggetto di notevole pubblicità⁴⁰⁾.

2. UTILIZZAZIONE DI CONTRATTI COME BASE PER FLUSSI INTRACOMUNITARI DI DATI

Prima di esaminare i requisiti delle disposizioni contrattuali nel contesto dei flussi di dati verso paesi terzi, occorre chiarire la differenza tra la situazione in un paese terzo e quella esistente all'interno della Comunità. In quest'ultimo caso, il contratto rappresenta il meccanismo utilizzato per definire e regolamentare la ripartizione delle responsabilità in materia di protezione dei dati ove più di un ente sia interessato al trattamento dei dati in questione. Ai sensi della direttiva un ente, il «responsabile del trattamento», deve assumersi la responsabilità principale per conformarsi ai principi essenziali di protezione dei dati. Il secondo ente, l'«incaricato del trattamento», è responsabile unicamente della sicurezza dei dati. Per responsabile del trattamento si intende un ente che abbia poteri decisionali circa le finalità e le modalità di trattamento dei dati, mentre l'incaricato del trattamento è unicamente l'ente che fornisce fisicamente il servizio di trattamento dei dati. La relazione tra i due enti è definita nell'articolo 17, paragrafo 3, della direttiva:

– l'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente: - che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento; - che gli obblighi di cui al paragrafo 1 (disposizioni essenziali riguardo alla sicurezza dei dati), quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.

Ciò deriva dal principio generale di cui all'articolo 16 in base al quale l'incaricato del trattamento o chiunque agisca sotto l'autorità del responsabile del trattamento non deve elaborare i dati personali, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali.

³⁹⁾ «Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum», studio effettuato congiuntamente dal Consiglio d'Europa, dalla Commissione delle Comunità europee e dalla Camera di commercio internazionale, Strasburgo, 2 novembre 1992.

⁴⁰⁾ Cfr. la presentazione di Alexander Dix del caso in questione in occasione dell'«International Data Protection and Privacy Commissioners' Conference», settembre 1996, Ottawa.

Anche nel caso di trasferimento di dati personali verso paesi terzi, in genere sarà coinvolta più di una parte. In questo caso la relazione è tra l'ente che trasferisce i dati (il «cedente») e l'ente che riceve i dati nel paese terzo (il «destinatario»). In questo contesto uno degli obiettivi del contratto dovrebbe essere quello di determinare le modalità di ripartizione della responsabilità in materia di protezione dei dati tra le due parti. Peraltro il contratto deve mirare anche ad altro, cioè a fornire garanzie supplementari alla persona interessata dal trattamento dei dati, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto a un complesso di norme vincolanti in materia di protezione dei dati, atte a garantire un livello adeguato di tutela.

3. OBIETTIVO DI UNA SOLUZIONE CONTRATTUALE

Nell'ambito del trasferimento verso paesi terzi, quindi, il contratto costituisce un mezzo per il responsabile del trattamento di fornire garanzie adeguate al momento di trasferire i dati al di fuori della Comunità (e quindi al di fuori della tutela prevista dalla direttiva, nonché dal contesto generale della legislazione comunitaria ⁴¹⁾) verso un paese terzo in cui il livello generale di protezione non sia adeguato. Per soddisfare tale funzione, una disposizione contrattuale deve compensare in modo soddisfacente la mancanza di un livello generale di protezione adeguata e comportare gli elementi essenziali di tutela che possono mancare in una qualsiasi situazione particolare.

4. REQUISITI SPECIFICI DI UNA SOLUZIONE CONTRATTUALE

Il punto di partenza per valutare il significato di «garanzie sufficienti» quali utilizzate all'articolo 26, paragrafo 2, è la nozione di «tutela adeguata» già elaborata in parte nel documento di discussione «Primi orientamenti ...» ⁴²⁾. Tale documento illustra una strategia consistente in una serie di principi fondamentali in materia di protezione dei dati nonché in tre ulteriori requisiti: che nella pratica sussista un buon livello di osservanza di tali principi, che siano forniti sostegno e assistenza alle persone interessate dal trattamento dei dati per l'esercizio dei propri diritti e che vi sia una riparazione adeguata alla parte lesa ove tali principi non vengano osservati.

(i) Norme essenziali in materia di protezione dei dati

Il primo requisito della soluzione contrattuale è, quindi, che le parti interessate al trasferimento dei dati siano obbligate a garantire l'applicazione del complesso di principi fondamentali in materia di protezione dei dati figuranti nel documento «Primi orientamenti» all'atto del trattamento dei dati trasferiti verso il paese terzo. Tali principi fondamentali sono:

⁴¹⁾ L'esercizio dei diritti in materia di tutela dei dati da parte di una persona fisica è facilitato nell'ambito del contesto giuridico generale della Comunità, come ad esempio dall'Accordo di Strasburgo (1977) circa la trasmissione di richieste di assistenza giuridica.

⁴²⁾ «Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza», documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997.

1) **il principio della finalità limitata:** i dati dovrebbero essere trattati per una finalità specifica e successivamente utilizzati o ulteriormente comunicati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trasferimento. Le uniche deroghe a tale norma sarebbero quelle necessarie in ogni società democratica per una delle ragioni elencate nell'articolo 13 della direttiva (ad esempio, sicurezza dello Stato, accertamento di infrazioni penali) ⁴³⁾;

2) **il principio della qualità e della proporzionalità:** i dati dovrebbero essere precisi e, se del caso, aggiornati. Essi dovrebbero essere adeguati, pertinenti e non andare al di là delle finalità per cui sono oggetto di trasferimento o di ulteriore trattamento;

3) **il principio della trasparenza:** la persona dovrebbe ricevere informazioni riguardanti la finalità del trattamento dei dati e l'identità del responsabile del trattamento nel paese terzo, nonché qualunque altra informazione necessaria ad assicurare una procedura equa. Le uniche deroghe consentite dovrebbero essere conformi all'articolo 13 della direttiva, o all'articolo 11, paragrafo 2, che consente alle organizzazioni che non hanno raccolto i dati direttamente dalla persona interessata di essere dispensate da tale disposizione se l'informazione della persona interessata si rivela impossibile o richiede sforzi sproporzionati;

4) **il principio della sicurezza:** il responsabile del trattamento dei dati dovrebbe adottare misure di sicurezza tecnica e organizzativa commisurate ai rischi che il trattamento presenta. Chiunque operi sotto l'autorità del responsabile del trattamento, compreso un incaricato del trattamento, si occupa del trattamento dei dati solo su istruzione del responsabile medesimo;

5) **i diritti di accesso, rettifica e opposizione:** la persona interessata dovrebbe avere il diritto di ottenere una copia di tutti i dati trattati che la riguardano, nonché il diritto di far rettificare i dati di comprovata inesattezza. In determinate situazioni, la persona interessata dovrebbe inoltre potersi opporre al trattamento dei dati che la riguardano. Le uniche deroghe a tali diritti dovrebbero essere conformi all'articolo 13 della direttiva;

6) **restrizioni ai successivi trasferimenti verso parti non firmatarie del contratto:** ulteriori trasferimenti dei dati personali dal destinatario verso terzi non dovrebbero essere consentiti, a meno di trovare un metodo contrattuale che vincoli i terzi in questione a fornire alle persone interessate le stesse garanzie di protezione dei dati.

Inoltre, in alcune situazioni, vanno applicati principi supplementari:

1) **dati sensibili:** se il trattamento riguarda categorie «sensibili» di dati (quelle elencate all'articolo 8), si dovrebbero porre in essere misure di salvaguardia supplementari, come ad esempio l'obbligo del consenso esplicito al trattamento da parte della persona interessata;

2) **commercializzazione diretta:** se il trasferimento dei dati avviene per finalità di commercializzazione diretta, la persona interessata dovrebbe essere in grado di decidere in qualsiasi momento l'esclusione dei dati che la riguardano da un simile impiego;

⁴³⁾ Occorre rilevare che le finalità statistiche e di ricerca scientifica sono in genere considerate compatibili, a condizione che siano offerte garanzie adeguate.

3) **decisioni individuali automatizzate**: se la finalità del trasferimento consiste nell'adozione di una decisione automatizzata ai sensi dell'articolo 15 della direttiva, l'individuo dovrebbe avere il diritto di conoscere la logica che muove tale decisione e si dovrebbero prendere altri provvedimenti per garantire la salvaguardia del suo interesse legittimo.

Nel contratto andrebbe specificato in modo dettagliato il metodo in base al quale il destinatario del trasferimento dei dati dovrebbe applicare tali principi (ad esempio, andrebbero specificate le finalità, le categorie di dati, i termini di conservazione, le misure di sicurezza, ecc.). In altre situazioni, ad esempio quando in un paese terzo la protezione dei dati è fornita nell'ambito di una legislazione generale di protezione dei dati simile a quella specificata nella direttiva, potrebbero essere presenti altri meccanismi atti a chiarire il modo in cui le norme di protezione dei dati si applicano nella pratica (codici di comportamento, notifica, funzione di consulenza dell'autorità di controllo). In una situazione contrattuale ciò non avviene, ed è quindi indispensabile, quando il trasferimento avviene in base a un contratto, specificare i dettagli.

(ii) Rendere efficaci le norme essenziali

Nel documento «Primi orientamenti ...» figurano tre criteri in base ai quali andrebbe valutata l'efficacia del sistema di protezione dei dati. In base a tali criteri, il sistema dovrebbe:

1) fornire un **buon livello di osservanza** delle norme (non esiste alcun sistema che possa garantire un'osservanza del 100%, anche se alcuni sistemi sono migliori di altri). Un buon sistema è in genere caratterizzato da un elevato grado di consapevolezza dei propri obblighi da parte dei responsabili del trattamento e dei propri diritti e mezzi per esercitarli da parte delle persone interessate. L'esistenza di sanzioni efficaci e deterrenti è importante per garantire il rispetto delle norme, come lo sono pure sistemi di verifica diretta da parte di autorità, revisori o funzionari indipendenti addetti alla protezione dei dati;

2) fornire **sostegno e assistenza alle persone interessate dal trattamento dei dati** nell'esercizio dei propri diritti. La persona dev'essere in grado di far valere i propri diritti tempestivamente e in modo efficace, senza costi proibitivi. A tal fine, occorre la presenza di un tipo di struttura o meccanismo che consenta un controllo indipendente dei reclami;

3) fornire una **riparazione adeguata** alla parte lesa, quando le norme non vengono osservate. Si tratta di un elemento chiave, che deve comportare un sistema che fornisca giudizi imparziali e che consenta il risarcimento dei danni e l'imposizione di sanzioni a seconda dei casi.

Nel valutare l'efficacia di una soluzione contrattuale vanno applicati gli stessi criteri. Si tratta chiaramente di una sfida difficile ma non impossibile. Occorre trovare un mezzo che possa compensare l'assenza di meccanismi di controllo e di imposizione e fornire sostegno, assistenza e, in ultima analisi, una riparazione adeguata alla persona interessata, anche se non firmataria del contratto.

Ognuno di questi aspetti va esaminato nei dettagli. Per facilitare l'analisi, essi vengono esaminati in ordine inverso.

Fornire una riparazione alla persona interessata

Fornire un ricorso legale alla persona interessata (ad esempio, il diritto di presentare un reclamo ad un arbitro indipendente che possa giudicare in merito e il diritto di ricevere se del caso una riparazione) tramite un contratto tra il «ce-

dente» e il «destinatario» dei dati non è una questione semplice. Molto dipenderà dalla natura della legislazione in materia di contratti prescelta come legge nazionale applicabile al contratto. Prevedibilmente la legge applicabile sarà in genere quella dello Stato membro in cui la parte cedente è insediata. In alcuni Stati membri la legislazione in materia di contratti consente l'istituzione di diritti di terzi, che invece non è possibile in altri Stati membri.

In genere, comunque, quanto più il destinatario è limitato per quanto riguarda la possibilità di scegliere le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, tanto maggiore è la sicurezza giuridica per la persona interessata. Tenendo presente che si sta trattando di casi di protezione generale inadeguata, la soluzione migliore sarebbe quella di specificare nel contratto le modalità secondo le quali il destinatario deve applicare i principi fondamentali in materia di protezione dei dati in modo così dettagliato che, in pratica, il destinatario del trasferimento in questione non ha alcun potere autonomo di decisione per quanto riguarda i dati trasferiti o il modo in cui essi vengono trattati successivamente. Il destinatario è tenuto ad agire soltanto dietro istruzioni del cedente e, anche se i dati potrebbero essere stati fisicamente trasferiti al di fuori dell'Ue, il controllo decisionale sui dati spetta sempre all'ente, insediato nella Comunità, che ha effettuato il trasferimento. In tal modo il cedente resta il responsabile del trattamento, mentre il destinatario è semplicemente un subappaltatore incaricato del trattamento. In questo caso, dato che il controllo dei dati è esercitato da un ente che risiede in uno Stato membro dell'Ue, la legislazione dello Stato membro in questione continuerà ad essere applicabile al trattamento effettuato nel paese terzo ⁴⁴⁾, e inoltre il responsabile del trattamento continuerà, ai sensi della legislazione di tale Stato membro, ad essere responsabile di eventuali danni cagionati da un trattamento illecito ⁴⁵⁾.

Questo tipo di accordo non è molto dissimile da quello stabilito dall'«Accordo inter-territoriale» che ha risolto il caso Citibank «Bahncard» menzionato in precedenza. In questo caso, l'accordo contrattuale fissava nei dettagli le disposizioni riguardanti il trattamento dei dati, in particolare quelle relative alla sicurezza dei dati, e ne vietava qualsiasi altra utilizzazione da parte del destinatario del trasferimento. Nell'accordo la legislazione tedesca veniva applicata al trattamento dei dati effettuato nel paese terzo, garantendo in tal modo un ricorso legale alle persone interessate ⁴⁶⁾.

Naturalmente si verificheranno casi in cui sarà impossibile avvalersi di tale soluzione. Potrebbe darsi che il destinatario del trasferimento non debba semplicemente fornire un servizio di trattamento dei dati al responsabile del trattamento insediato nell'Ue, ma abbia, ad esempio, noleggiato o acquistato i dati per utilizzarli per i propri interessi o i propri scopi. In tali circostanze il destinatario dovrà disporre di una certa libertà nel trattamento dei dati, diventando in pratica a tutti gli effetti un «responsabile del trattamento» dei dati.

⁴⁴⁾ Ai sensi dell'art. 4, paragrafo 1, lettera a), della direttiva 95/46/CE.

⁴⁵⁾ Cfr. art. 23 della direttiva 95/46/CE.

⁴⁶⁾ Peraltro, dato che il caso è sopravvenuto nell'ambito di una legislazione precedente alla direttiva, la legislazione stessa non è stata applicata automaticamente a tutti i trattamenti controllati da un responsabile del trattamento insediato in Germania. Il ricorso legale per le persone interessate è stato invece possibile grazie alla legislazione contrattuale tedesca che consente di istituire diritti di terzi.

In casi del genere non è possibile fare affidamento sull'applicabilità automatica permanente della legislazione di uno Stato membro e sulla responsabilità permanente del cedente per eventuali danni causati. Per fornire alle persone interessate un adeguato ricorso legale vanno concepiti altri meccanismi più complessi. Come detto in precedenza, alcuni sistemi giuridici consentono a terzi la rivendicazione di diritti nell'ambito di un contratto, e questa possibilità potrebbe essere utilizzata per istituire i diritti delle persone interessate grazie ad un contratto pubblico e pubblicato tra il cedente e il destinatario. La posizione delle persone interessate verrebbe ulteriormente rafforzata ove, come parte del contratto, le parti si impegnassero a sottoporsi ad una specie di arbitrato vincolante qualora una persona interessata dal trattamento dei dati contestasse la loro osservanza. Alcuni codici di autodisciplina settoriale includono tali meccanismi di arbitrato, e potrebbe essere utile prevedere l'utilizzazione di contratti abbinata a tali codici.

Un'altra possibilità consiste nello stipulare, eventualmente al momento dell'ottenimento iniziale dei dati, un accordo contrattuale a parte tra il cedente e la persona interessata dal trattamento dei dati, in base al quale il cedente rimarrebbe responsabile di eventuali danni o difficoltà causate dall'inosservanza, da parte del destinatario del trasferimento dei dati, dell'insieme convenuto di principi fondamentali in materia di protezione dei dati. In questo modo la persona interessata ha la garanzia di un ricorso contro il cedente per le infrazioni del destinatario. Spetterebbe allora al cedente ottenere il risarcimento dei danni pagati alla persona interessata, intentando causa al destinatario per inadempienza contrattuale.

Una soluzione a tre così complessa è forse più attuabile di quanto possa sembrare a prima vista. Il contratto con la persona interessata potrebbe diventare parte integrante delle condizioni generali tipo in base alle quali una banca o un'agenzia di viaggi, ad esempio, fornisce servizi ai clienti, presentando inoltre il vantaggio della trasparenza: la persona interessata è pienamente cosciente dei suoi diritti.

Infine, come alternativa a un contratto con la persona interessata, si potrebbe prospettare la possibilità, per uno Stato membro, di disporre per legge una responsabilità permanente dei responsabili del trattamento che trasferiscono dati al di fuori della Comunità per quanto riguarda eventuali danni causati dalle azioni del destinatario del trasferimento.

Fornire sostegno e assistenza alle persone interessate dal trattamento dei dati

Una delle principali difficoltà cui devono far fronte le persone i cui dati vengono trasferiti verso una giurisdizione straniera è quello di essere incapaci di scoprire la causa originaria del problema particolare che le affligge e di trovarsi quindi nell'incapacità di giudicare se le norme di protezione dei dati siano state correttamente osservate oppure se sussistano motivi di ricorso legale⁴⁷⁾. Per un livello di tutela adeguato è quindi necessario un certo tipo di meccanismo istituzionale che possa indagare sui reclami.

⁴⁷⁾ Anche se i diritti delle persone interessate sono stati garantiti nell'ambito di un contratto, tali persone spesso non saranno in grado di giudicare se si sia verificata un'inadempienza contrattuale e da parte di chi. È quindi necessaria una procedura investigativa al di fuori delle procedure legali del diritto civile ufficiale.

Il controllo e la funzione investigativa dell'autorità di controllo di uno Stato membro si limitano al trattamento dei dati effettuato nel territorio dello Stato membro in questione⁴⁸⁾. Quando i dati vengono trasferiti verso un altro Stato membro, un sistema di assistenza reciproca tra le autorità di controllo garantisce che un eventuale reclamo di una persona interessata nel primo Stato membro venga sottoposto ad un'indagine adeguata. Quando invece il trasferimento è effettuato verso un paese terzo, nella maggior parte dei casi tale garanzia non esiste. Si tratta quindi di esaminare che tipo di meccanismo di compensazione possa essere adottato nel contesto di un trasferimento di dati sulla base di un contratto.

Una possibilità potrebbe essere quella di esigere semplicemente una clausola contrattuale che garantisca all'autorità di controllo dello Stato membro in cui è insediato il cedente il diritto di controllare il trattamento effettuato dall'incaricato del trattamento nel paese terzo. Nella pratica, tale controllo potrebbe essere effettuato da un agente (ad esempio, una società di certificazione specializzata) designato dall'autorità di controllo, ove necessario. Una difficoltà inerente a un metodo del genere, tuttavia, consiste nel fatto che l'autorità di controllo in genere⁴⁹⁾ non è parte firmataria del contratto e, di conseguenza, in alcune giurisdizioni potrebbe non avere i mezzi di appellarsi ad esso per avere accesso. Un'altra possibilità potrebbe essere un obbligo legale fornito dal destinatario nel paese terzo direttamente all'autorità di controllo dello Stato membro dell'Ue interessato, in base al quale il destinatario dei dati autorizza l'accesso all'autorità di controllo o a un agente designato qualora sorgessero sospetti di inadempienza dei principi in materia di protezione dei dati. Tale obbligo potrebbe anche richiedere alle parti interessate dal trasferimento dei dati di informare l'autorità di controllo circa qualsiasi reclamo ricevuto dalle persone interessate dal trattamento dei dati. Ai sensi di tale accordo tale obbligo sarebbe una condizione da soddisfare prima dell'autorizzazione al trasferimento dei dati.

Indipendentemente dalla soluzione prescelta, permangono tuttavia seri dubbi quanto all'opportunità, praticità o invero fattibilità, da un punto di vista delle risorse, di assumersi - da parte di un'autorità di controllo di uno Stato membro dell'Ue - la responsabilità di esaminare e controllare il trattamento di dati effettuato in un paese terzo.

Fornire un buon livello di osservanza

Anche in mancanza di un particolare reclamo o difficoltà riscontrata da una persona interessata dal trattamento dei dati, è indispensabile un elevato grado di fiducia nell'osservanza delle condizioni contrattuali da parte dei firmatari. Il problema con la soluzione contrattuale consiste nella difficoltà di fissare sanzioni per inosservanza del contratto che siano sufficientemente significative e ottenere l'effetto deterrente necessario per garantire tale fiducia. Anche qualora un controllo efficace dei dati continuasse ad essere esercitato dall'interno della Comunità, il destinatario del trasferimento potrebbe non incorrere in alcuna sanzione penale diretta, anche se il trattamento dei dati avvenisse in violazione del contratto. La responsabilità incomberebbe invece al cedente insediato nella

⁴⁸⁾ Cfr. art. 28, paragrafo 1, della direttiva 95/46/CE.

⁴⁹⁾ Secondo la delegazione francese potrebbero verificarsi situazioni in cui l'autorità di controllo è parte firmataria del contratto.

Comunità, che dovrebbe poi ottenere il risarcimento di eventuali danni intendendo una causa a parte contro il destinatario. Una responsabilità indiretta del genere potrebbe non essere sufficiente a indurre il destinatario all'osservanza di tutti i dettagli del contratto.

Stando così le cose, è probabile che nella maggior parte dei casi una soluzione contrattuale dovrà essere integrata da quanto meno la possibilità di una qualche forma di controllo esterno delle attività di trattamento del destinatario, ad esempio una verifica effettuata da un ente di normalizzazione o da una società di certificazione specializzata.

5. IL PROBLEMA DELLA LEGGE DIRIMENTE

Una difficoltà particolare insita nel metodo contrattuale è la possibilità che la legislazione generale del paese terzo contempli l'obbligo, per il destinatario del trasferimento dei dati, di rivelare - in determinati casi - dati personali alle autorità pubbliche (polizia, tribunali o fisco, ad esempio) e che tali obblighi legali abbiano la precedenza su qualsiasi contratto che l'incaricato del trattamento abbia sottoscritto⁵⁰⁾. Per gli incaricati del trattamento all'interno della Comunità questa possibilità figura all'articolo 16 della direttiva, secondo cui l'incaricato del trattamento può elaborare i dati solo dietro istruzione del responsabile del trattamento oppure *in virtù di obblighi legali*. Ai sensi della direttiva, peraltro, la rivelazione di informazioni (che sia per sua stessa natura per finalità incompatibili con quelle per le quali i dati sono stati raccolti) va limitata al minimo necessario in società democratiche e per uno dei motivi di «ordine pubblico» di cui all'articolo 13, paragrafo 1, della direttiva. Anche l'articolo 6 del trattato di Amsterdam garantisce il rispetto dei diritti fondamentali stabiliti nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. In paesi terzi non sempre potrebbero esistere analoghe limitazioni per i poteri pubblici di ottenere dati personali da società e da altre organizzazioni operanti sul loro territorio.

Non esiste un metodo facile per superare tale difficoltà, da cui si evincono chiaramente le limitazioni del metodo contrattuale. In alcuni casi il contratto è uno strumento troppo fragile per offrire garanzie adeguate di protezione dei dati, e non andrebbero autorizzati trasferimenti verso certi paesi.

6. CONSIDERAZIONI PRATICHE IN MERITO ALL'UTILIZZAZIONE DI CONTRATTI

Dall'analisi precedente si è visto che qualsiasi soluzione contrattuale deve essere particolareggiata e opportunamente adeguata al trasferimento di dati in questione. Questo bisogno di dettaglio, per quanto riguarda le finalità e le condizioni precise di trattamento dei dati trasferiti, non esclude la possibilità di elaborare un modello di contratto tipo che però, per ogni contratto, andrà completato in modo da adeguarlo alle circostanze particolari del caso.

⁵⁰⁾ La portata dei poteri pubblici per quanto concerne l'obbligo di rivelare informazioni è un aspetto di cui tener conto anche al momento di una valutazione più generale dell'adeguatezza della tutela in un paese terzo.

L'analisi ha inoltre dimostrato che esistono difficoltà pratiche particolari nell'indagine dell'inosservanza di un contratto quando il trattamento avviene al di fuori dell'Ue e ove il paese terzo in questione non fornisca alcuna forma di autorità di controllo. Insieme, queste due considerazioni significano che si verificeranno alcune situazioni in cui la soluzione contrattuale potrebbe essere la soluzione adeguata, mentre in altre situazioni potrebbe essere impossibile fornire per contratto le necessarie «garanzie sufficienti».

Vista l'esigenza di un adeguamento particolareggiato di un contratto alle peculiarità del trasferimento in questione, un contratto è particolarmente adatto in situazioni in cui i trasferimenti di dati sono simili e di natura ripetitiva. Date le difficoltà inerenti al controllo, una soluzione contrattuale potrebbe essere maggiormente efficace quando le parti firmatarie del contratto sono rappresentate da operatori importanti già sottoposti a sorveglianza e regolamentazione pubblica⁵¹⁾. Le grandi reti internazionali, ad esempio quelle utilizzate per le transazioni nel campo delle carte di credito e per le prenotazioni aeree, presentano entrambe queste caratteristiche e fanno riscontrare situazioni in cui i contratti si potrebbero rivelare estremamente utili. In queste circostanze, essi potrebbero addirittura essere integrati da convenzioni multilaterali intese a fornire una migliore sicurezza giuridica. Allo stesso modo, quando le parti interessate dal trasferimento sono affiliate o formano parte dello stesso gruppo di imprese, la capacità di indagare in merito all'inosservanza di un contratto è presumibilmente molto rafforzata, dati gli stretti legami tra il destinatario nel paese terzo e l'ente insediato nella Comunità. I trasferimenti intra-aziendali costituiscono pertanto un altro settore che presenta un chiaro potenziale per lo sviluppo di soluzioni contrattuali efficaci.

Conclusioni e raccomandazioni principali

– Nell'ambito della Comunità i contratti vengono utilizzati come mezzo per stabilire la ripartizione delle responsabilità in materia di osservanza della protezione dei dati tra il responsabile del trattamento e il subappaltatore incaricato del trattamento. Un contratto utilizzato per flussi di dati verso paesi terzi deve fare molto di più: fornire garanzie supplementari alle persone interessate dal trattamento dei dati, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto a un complesso di norme vincolanti in materia di protezione dei dati atte a fornire un livello di tutela adeguato.

– La base per la valutazione dell'adeguatezza delle garanzie fornite da una soluzione contrattuale è la stessa che per la valutazione del livello generale di adeguatezza in un paese terzo. Una soluzione contrattuale deve comprendere tutti i principi fondamentali in materia di protezione dei dati e fornire mezzi con cui rendere applicabili tali principi.

– Nel contratto andrebbero specificati in dettaglio le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, nonché le modalità di applicazione dei principi fondamentali in materia di protezione dei dati. Una maggiore sicurezza giuridica è fornita da contratti in cui viene limitata la libertà del destinatario dei dati di trattare questi ultimi in modo autonomo per proprio conto. Il con-

⁵¹⁾ Nel caso Citibank «Bahncard» il sovrintendente alla tutela dei dati di Berlino ha cooperato con le autorità di controllo bancario americane.

tratto andrebbe quindi utilizzato, nei limiti del possibile, come mezzo con cui l'ente che trasferisce i dati mantiene il controllo decisionale sul trattamento effettuato nel paese terzo.

– Ove il destinatario abbia un certo grado di autonomia quanto al trattamento dei dati trasferiti, la situazione non è chiara, e un solo contratto tra le parti interessate al trasferimento può non sempre costituire una base sufficiente per l'esercizio dei diritti da parte delle persone interessate dal trattamento dei dati. Potrebbe essere necessario un meccanismo in base al quale la parte insediata nella Comunità che provvede al trasferimento resta responsabile di eventuali danni causati dal trattamento effettuato nel paese terzo.

– I trasferimenti successivi verso enti o organizzazioni non legate dal contratto andrebbero specificatamente esclusi dal contratto in questione, a meno che non sia possibile vincolare per contratto tali terzi a rispettare gli stessi principi in materia di protezione dei dati.

– Il grado di fiducia nel rispetto dei principi in materia di protezione dei dati dopo il trasferimento dei dati stessi verrebbe rafforzato se l'osservanza dei principi di protezione dei dati da parte del destinatario del trasferimento fosse sottoposta ad una verifica esterna da parte, ad esempio, di una società di certificazione specializzata o di un istituto di normalizzazione.

– Qualora una persona interessata dal trattamento dei dati incontrasse un problema derivante eventualmente da una violazione delle disposizioni in materia di protezione dei dati garantite nel contratto, il problema generale è quello di garantire che il reclamo della persona interessata venga adeguatamente esaminato. Le autorità di controllo degli Stati membri dell'Ue riscontreranno difficoltà pratiche nell'effettuare tale controllo.

– Le soluzioni contrattuali sono probabilmente più adatte a grandi reti internazionali (carte di credito, prenotazioni aeree) caratterizzate da notevoli quantità di trasferimenti di dati ripetitivi di natura simile e da un numero relativamente esiguo di importanti operatori in settori industriali già sottoposti ad un elevato grado di controllo e di regolamentazione pubblica. I trasferimenti intra-aziendali di dati tra varie branche dello stesso gruppo di imprese è un altro settore in cui esiste un notevole potenziale per l'utilizzazione dei contratti.

– I paesi in cui i poteri delle autorità pubbliche in materia di accesso alle informazioni superano quelli consentiti dalle norme internazionalmente accettate in materia di tutela dei diritti dell'uomo non rappresentano destinazioni sicure per i trasferimenti basati su clausole contrattuali.

Fatto a Bruxelles, il 22 aprile 1998

Per il gruppo di lavoro
Il presidente P.J. HUSTINX

5.7.3 Raccomandazione 1/98 in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni, diritto delle società ed informazione finanziaria

Libera circolazione delle informazioni e protezione dei dati, compresi gli aspetti internazionali

XV/ D/5009/98 def.
WP 10

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 1/98 in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo

adottata dal Gruppo il 28 aprile 1998

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 ⁵²⁾,

Visto l'articolo 29 e l'articolo 30, paragrafo 3 della menzionata direttiva,

Visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

1. INTRODUZIONE

L'articolo 6, paragrafo 1, lettera *b*) della direttiva 95/46 impone agli Stati membri di disporre che i dati personali siano «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità»; a norma del § 1, lettera *e*) del medesimo articolo, i dati devono essere «conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati».

⁵²⁾ GU L 281 del 23.11.1995, pag. 31.

L'art. 8 della direttiva impone agli Stati membri di vietare il trattamento di dati personali che rivelino, tra l'altro, l'origine razziale o etnica, le convinzioni religiose e le condizioni di salute. Sono ammesse deroghe a questo principio per i motivi specificati nell'art. 8, paragrafi 2 e 3, ed uno di tali motivi è costituito dal consenso esplicito della persona interessata.

Ai sensi della direttiva la persona interessata gode di specifici diritti, compreso il diritto di essere informato circa il trattamento dei suoi dati personali (articoli 10 e 11), nonché i diritti di accesso, di rettifica e di cancellazione (art. 12).

In considerazione degli aspetti peculiari alle prenotazioni nel trasporto aereo e delle recenti iniziative della Commissione in tale settore⁵³⁾, il Gruppo ha deciso di creare un sottogruppo in materia di sistemi telematici di prenotazione (CRS). Esso si è riunito due volte ed ha stabilito di presentare al Gruppo gli esiti dei suoi lavori in vista dell'adozione della presente raccomandazione.

2. RELAZIONE

Il settore del trasporto aereo è caratterizzato da un uso estremamente avanzato di sistemi informatici. Esistono banche dati contenenti dati personali in molti ambiti: in particolare presso le compagnie aeree, gli agenti di viaggio ed i sistemi telematici di prenotazione (CRS). Diverse banche dati (in particolare, ma non esclusivamente, i CRS) sono ubicate al di fuori del territorio della Comunità.

In considerazione della natura internazionale del trasporto aereo, le soluzioni di carattere generale sono, in linea di principio, le più appropriate.

Il Gruppo ritiene che i seguenti aspetti meritino di essere considerati in via prioritaria:

1. Informazione e diritto di accesso:

– La grande maggioranza dei dati personali viene raccolta dagli agenti di viaggio e dai vettori aerei. Per motivi pratici, e senza pregiudizio della definizione di «responsabile del trattamento» ai sensi della direttiva 95/46/CE, la questione del diritto di accesso della persona interessata dovrebbe pertanto investire in primis tali operatori.

– Tuttavia, taluni aspetti relativi all'accesso possono anche essere regolamentati direttamente assieme ai CRS, e ciò potrebbe avvenire nel progetto di regolamento relativo al codice di comportamento per i CRS proposto dalla Commissione.

– Il codice di comportamento in materia di sistemi telematici di prenotazione ribadisce il diritto dei passeggeri di essere informati in modo dettagliato circa il trattamento dei dati. Tale diritto potrebbe essere rafforzato attraverso il coinvolgimento degli abbonati (ad esempio gli agenti di viaggio) e dei vettori aerei.

2. Cancellazione di dati:

– È auspicabile assicurare che i dati personali siano cancellati dai sistemi computerizzati di prenotazione non appena cessino di essere utilizzati ai fini del viaggio.

⁵³⁾ Proposta di regolamento (CE) del Consiglio che modifica il regolamento (CEE) n. 2299/89 del Consiglio relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione (CRS); COM (97) 246 def. del 9 luglio 1997.

– Mentre tali dati possono servire nel caso di contenzioso e pertanto potrebbe risultare necessario conservarli per un certo periodo di tempo, essi dovrebbero essere utilizzati soltanto a tale fine specifico ed essere successivamente distrutti.

– Ciò non pregiudica la possibilità che gli abbonati ed i vettori aerei ottengano il consenso da parte di viaggiatori abituali al fine del trattamento dei loro dati personali in conformità della direttiva 95/46/CE.

3. CONCLUSIONI

In considerazione di quanto precede, il Gruppo raccomanda che:

– La proposta di regolamento che modifica il regolamento (CEE) n. 2299/89 del Consiglio relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione (CRS) sia integrata prevedendo:

– Il preciso obbligo di fornire **informazioni** al cliente circa il trattamento dei dati personali nel sistema telematico. Tali informazioni, che possono essere diffuse ad esempio con opuscoli illustrativi, dovrebbero includere il nome e l'indirizzo del venditore del sistema, gli scopi del trattamento dei dati, il periodo di conservazione degli stessi, nonché le modalità e gli strumenti necessari per l'esercizio del diritto di accesso da parte della persona interessata.

– L'obbligo per gli abbonati (ad esempio, agenti di viaggio) ed i vettori aerei di ottenere dalle persone interessate l'esplicito consenso alla raccolta di dati di natura delicata (condizione di disabile, pasti conformi ai precetti islamici, ecc.). Qualora il CRS includa la possibilità di emissione diretta di biglietti, tale obbligo deve essere applicato al venditore del sistema ⁵⁴⁾.

– L'obbligo delle parti citate di rispondere immediatamente ad una richiesta di **accesso** da parte di un passeggero che desideri prendere visione dei propri dati.

– L'obbligo per il CRS di assicurare che tutti i dati personali identificati siano archiviati fuori linea entro le 72 ore successive al termine del viaggio in questione ⁵⁵⁾ e distrutti entro un periodo non superiore ai tre anni. L'accesso a tali dati dovrà essere consentito soltanto ai fini della composizione di controverse relative alla fatturazione. Nonostante l'obbligo di distruggere i dati entro tre anni, i dati personali possono essere conservati per un periodo più lungo e per tutto il tempo necessario nel caso specifico al fine di espletare una richiesta di indennizzo per danni ovvero per il periodo stabilito da disposizioni di legge (ad esempio, le disposizioni in materia contabile e fiscale).

– L'obbligo di effettuare le necessarie modifiche al fine di estendere l'ambito di applicazione del controllo previsto dall'art. 21 bis.

– Inoltre, il Gruppo raccomanda che vengano presi in esame in via prioritaria gli specifici problemi sollevati dalle prenotazioni in linea che non rientrano nell'ambito di applicazione del CRS (ad esempio, agenti di viaggio o vettori aerei che propongono l'acquisto diretto di biglietti via Internet) e che la Commis-

⁵⁴⁾ Secondo la definizione contenuta nel citato codice di comportamento, si intende per «venditore del sistema» «qualsiasi impresa e le sue affiliate che provveda alla gestione o commercializzazione di un CRS».

⁵⁵⁾ Come indicato nella relazione, rimane impregiudicato il diritto degli abbonati e dei vettori aerei di trattare i dati di natura delicata relativi ai viaggiatori abituali nei propri sistemi informatici, dietro consenso esplicito della persona interessata.

sione proponga con urgenza delle soluzioni appropriate. A tale proposito, invita la Commissione a precisare se tale aspetto è disciplinato dalla direttiva 97/66/CE ⁵⁶⁾ ed in che misura.

La presente raccomandazione, adottata dal Gruppo in data 28 aprile 1998, è rivolta alla Commissione europea, al Parlamento europeo, al Consiglio dell'Unione europea ed al Comitato economico e sociale.

Fatto a Bruxelles, addì 28 aprile 1998

Per il Gruppo
Il Presidente P.J. HUSTINX

⁵⁶⁾ Direttiva 97/66/CE del Parlamento Europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (GU L 24 del 30.1.1998, pag. 1).

5.7.4 Parere n. 1/98: preferenze in materia di protezione della vita privata e la «norma aperta per i profili»

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni - Diritto delle società e informazione finanziaria

Libera circolazione delle informazioni, tutela dei dati e relativi aspetti internazionali

XV D/5032/98
WP 11

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Parere n. 1/98: Piattaforma per le preferenze in materia di protezione della vita privata (P3P - *Platform for Privacy Preferences*) e la «norma aperta per i profili» (OPS - *Open Profiling Standard*)

Adottato dal gruppo il 16 giugno 1998

PARERE DEL GRUPPO

Il progetto della piattaforma per le preferenze in materia di protezione della vita privata (P3P - *Platform for Privacy Preferences*) considera la tutela della vita privata e dei dati personali come un elemento che deve essere stabilito di comune accordo fra l'utente Internet di cui si raccolgono i dati ed il sito Web che li registra. Il principio di base prevede che l'utente acconsenta alla raccolta dei suoi dati personali da parte di un sito (l'*Open Profiling Standard* è volto a fornire la trasmissione sicura di un profilo standard di dati personali), solo se le pratiche dichiarate del sito in termini di protezione della vita privata (per esempio le finalità della raccolta dei dati, l'eventuale uso a fini secondari o la cessione a terzi) soddisfano le esigenze dell'utente. Il World Wide Web Consortium ha cercato di elaborare un unico vocabolario che permettesse di esprimere le preferenze dell'utente e le pratiche del sito. Non è prevista la possibilità di adattare questo vocabolario alle esigenze e al quadro normativo di regioni geografiche specifiche. Sorprende il fatto che, malgrado la prevista applicabilità universale della P3P, il suddetto vocabolario non sia stato messo a punto facendo riferimento alle norme conosciute di livello più elevato nella protezione dei dati personali e della vita privata, ma si limiti a formalizzare norme comuni di livello inferiore. Queste decisioni di strategia fanno sì che l'applicazione della P3P e dell'OPS in seno all'Unione europea abbia buone probabilità di sollevare una serie di problemi specifici, discussi più avanti. Affinché la P3P e l'OPS abbiano ricadute positive sulla protezione della vita privata «in linea», è di fondamentale importanza che siano affrontati questi argomenti.

– Una piattaforma tecnica per la protezione della vita privata non sarà di per sé sufficiente a garantire tale protezione sul Web. Occorre che una piattaforma del genere sia applicata in un quadro di regole esecutive sulla tutela dei dati, in

grado di fornire a tutti un livello minimo e non negoziabile di protezione della vita privata. L'utilizzazione della P3P e dell'OPS senza questo quadro di riferimento rischia di scaricare principalmente sul singolo utente l'onere della protezione; si tratterebbe di un'evoluzione contraria alla norma ormai consolidata a livello internazionale secondo cui il «responsabile del trattamento» deve rispettare i principi della tutela dei dati (orientamenti OCSE del 1980, convenzione n. 108 del 1981 del Consiglio d'Europa, orientamenti ONU del 1990, direttive Ue 95/46/CE e 97/66/CE). Tale inversione di responsabilità presuppone peraltro un livello di conoscenza dei rischi per la vita privata posti dal trattamento dei dati che la maggioranza dei cittadini probabilmente non possiede.

– Esiste il rischio che la P3P, una volta applicata alla prossima generazione di software per il *browsing*, possa far erroneamente ritenere a taluni «incaricati del trattamento» con sede nell'Ue di poter essere esentati da determinati obblighi giuridici (per esempio, la concessione ai singoli utenti del diritto di accesso ai loro dati), qualora il singolo utente vi acconsenta nell'ambito della negoziazione «in linea». In realtà, le imprese, le organizzazioni e i singoli cittadini stabiliti nell'Ue e fornitori di servizi su Internet dovranno comunque osservare le norme fissate nella direttiva 95/46/CE sulla tutela dei dati (come recepita nella legislazione nazionale) per quanto riguarda la raccolta ed il trattamento dei dati personali. La P3P potrebbe pertanto essere fonte di confusione non solo tra gli incaricati del trattamento riguardo ai loro obblighi, ma anche tra gli utenti di Internet riguardo alla natura dei loro diritti in termini di protezione dei dati. Il software per il *browsing* venduto o distribuito nell'Ue deve pertanto essere progettato e configurato in modo tale da assicurare l'impossibilità di concludere accordi «in linea» che violino la normativa prevalente in materia di tutela dei dati.

– Per l'utente che ha sede nell'Ue ed entra in contatto con siti Web stabiliti in paesi non comunitari la preoccupazione principale deriva dal fatto che le organizzazioni a cui fornisce i suoi dati personali potrebbero non essere soggette alla direttiva Ue o a qualunque altra normativa che disciplini in modo efficace la protezione dei dati⁵⁷⁾. Per decidere se fornire o meno i dati a questi siti, sarà di fondamentale importanza sapere non solo quale sia il contenuto approssimativo di tutte le regole applicabili, ma anche se esistono sanzioni in caso di inosservanza, in particolare se è previsto uno strumento semplice ed efficace di ricorso nei casi di violazione. Una piattaforma «in linea» per le preferenze in materia di protezione della vita privata dovrebbe in teoria essere in grado di fornire tali informazioni agli utenti. Tuttavia, la configurazione attuale del vocabolario della P3P non richiede né prevede che agli utenti siano fornite informazioni circa le sanzioni o i ricorsi. Risulta pertanto necessario rivedere il vocabolario standard, affinché la P3P possa rivelarsi uno strumento utile per ottenere «in linea» dagli utenti Ue un consenso informato al trasferimento di dati personali (secondo quanto disposto dall'articolo 26, paragrafo 1, lettera a), della direttiva).

– Essendo improbabile che la maggior parte degli utenti Internet cambi anche uno solo dei parametri predeterminati sul proprio *browser*, la configurazione predefinita (*default*) relativa alle preferenze dell'utente in materia di prote-

⁵⁷⁾ Resta impregiudicata la possibilità di un esame dettagliato dell'articolo 4 della direttiva 95/46/CE, che potrebbe essere interpretato in maniera tale da rendere la direttiva applicabile a siti di paesi terzi che raccolgano dati da utenti con sede nell'Ue.

zione della vita privata avrà un'influenza decisiva sul livello complessivo della protezione della vita privata «in linea». La P3P e l'OPS devono essere applicate nella tecnologia dei *browser* con posizioni di *default* che rispecchino l'interesse dell'utente a beneficiare di un livello elevato di protezione della vita privata (compresa la possibilità di esplorare dei siti Web mantenendo l'anonimato) senza trovarsi bloccato o infastidito nei suoi tentativi di accedere ad un sito. Se l'incaricato del trattamento pone come condizione di accesso al proprio sito la fornitura di un profilo di dati identificabili, l'utente dovrebbe essere interrogato ogni volta se intende acconsentire alla fornitura di tali informazioni al sito in questione. Se il sito non richiede questi dati in via preliminare, l'accesso dovrebbe procedere senza interruzioni. I principali produttori di software per il *browsing* hanno la responsabilità di applicare la P3P e l'OPS in modo da rinforzare piuttosto che ridurre i livelli di protezione della vita privata.

Data l'importanza del processo di applicazione della P3P e dell'OPS, e alla luce dei diversi temi attualmente allo studio del gruppo relativamente alla funzionalità dei protocolli Web (HTTP), il gruppo è favorevole all'elaborazione di software Internet conformemente alla normativa sulla tutela dei dati applicabile nell'Unione europea e ritiene opportuna la messa a punto di meccanismi in grado di verificare la conformità del software Internet a tale riguardo.

Fatto a Bruxelles, il 16 giugno 1998

Per il Gruppo
Il Presidente P.J. HUSTINX

5.7.5 Trasferimento di dati personali verso Paesi terzi

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni - Diritto delle società e informazione finanziaria

Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

DG XV D/5025/98

WP 12

Gruppo di lavoro «Tutela delle persone fisiche
con riguardo al trattamento dei dati personali»

**Documento di lavoro: Trasferimento di dati personali verso paesi terzi:
applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei
dati**

Approvato dal gruppo di lavoro il 24 luglio 1998

INTRODUZIONE

Il presente documento, basato sui lavori del gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29 della direttiva sulla protezione dei dati (95/46/CE)⁵⁸⁾, si propone di esaminare in modo organico tutte le principali questioni poste dal trasferimento di dati personali verso paesi terzi nel contesto dell'applicazione della direttiva europea sulla protezione dei dati. Il documento è strutturato secondo il sistema previsto dagli articoli 25 e 26 della direttiva per i trasferimenti internazionali di dati personali. (Il testo degli articoli è riportato nell'allegato 2).

L'articolo 25, paragrafo (1), stabilisce che gli Stati membri possono consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo in questione garantisce un livello di protezione adeguato. Il paragrafo (2) precisa che la «adeguatezza» è valutata di volta in volta «con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati». Il paragrafo (6) prevede che la Commissione possa determinare che un paese terzo garantisce un livello di protezione adeguato. Il **capitolo 1** del pre-

⁵⁸⁾ Cfr **WP 4 (5020/97)** «Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza», documento di consultazione approvato dal gruppo di lavoro il 26 giugno 1997;

WP 7 (5057/97) Documento di lavoro: «Valutazione dell'autodisciplina settoriale: quando incide in modo significativo sul livello di tutela dei dati in un paese terzo?», approvato dal gruppo di lavoro il 14 gennaio 1998;

WP 9 (5005/98) Documento di lavoro: «Pareri preliminari circa l'utilizzazione di disposizioni contrattuali nel contesto del trasferimento di dati personali verso paesi terzi», approvato dal gruppo di lavoro il 22 aprile 1998.

sente documento esamina la questione centrale della protezione adeguata; si propone di chiarire che cosa si intenda per «adeguata» e definisce una serie di criteri in base a cui valutare, in un caso specifico, l'adeguatezza della protezione.

I capitoli 2 e 3 sono dedicati all'applicazione di questi criteri. Il **capitolo 2** tratta dei trasferimenti verso i paesi che hanno ratificato la convenzione n. 108 del Consiglio d'Europa; il **capitolo 3** esamina le questioni attinenti ai trasferimenti per i quali la protezione dei dati personali è assicurata principalmente o esclusivamente da meccanismi di autodisciplina e non da norme di legge.

In caso di mancanza di una protezione adeguata ai sensi dell'articolo 25, paragrafo 2, la direttiva prevede all'articolo 26, paragrafo 2 la possibilità di provvedimenti *ad hoc*, in particolare di natura contrattuale, tali da fornire garanzie sufficienti per autorizzare un trasferimento di dati personali. Nel **capitolo 4** sono esaminate le circostanze in cui possono essere appropriate soluzioni contrattuali *ad hoc* e sono formulate alcune raccomandazioni quanto alla forma e al contenuto possibili di tali soluzioni.

Il **capitolo 5** tratta della terza ed ultima situazione contemplata dalla direttiva: i casi specifici, previsti dall'articolo 26, paragrafo (1), nei quali è possibile derogare ai principi della «tutela adeguata». Viene esaminata l'esatta portata di tali deroghe, con alcune esemplificazioni di casi in cui tali deroghe potrebbero o no applicarsi.

Infine, il **capitolo 6** contiene alcuni commenti su questioni procedurali relative alla valutazione dell'adeguatezza (o inadeguatezza) della protezione e all'adozione di un approccio comunitario coerente a tali questioni.

I casi esaminati nell'allegato 1 si propongono di esemplificare l'applicazione concreta dell'approccio illustrato nel presente documento.

1. VALUTAZIONE DELLA TUTELA ADEGUATA

1) In che cosa consiste una «tutela adeguata»?

Proteggere i dati significa proteggere la persona alla quale si riferiscono le informazioni trattate. A tal fine si associano in genere una serie di diritti di cui gode la persona interessata e una serie di obblighi a carico di chi tratta i dati e che controlla tale trattamento. Gli obblighi e i diritti istituiti dalla direttiva 95/46/CE si basano su quelli stabiliti nella convenzione n. 108 (1981) del Consiglio d'Europa, che a loro volta non si discostano da quelli contenuti negli orientamenti dell'OCSE (1980) o dell'ONU (1990). Sembra pertanto esistere un consenso circa il contenuto delle norme di tutela dei dati che si estende ben oltre i quindici Stati membri della comunità.

Tali norme, tuttavia, contribuiscono alla tutela dell'individuo solo se sono osservate nella pratica. È pertanto necessario considerare non soltanto il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo, ma anche i meccanismi posti in essere per garantirne l'efficacia. In Europa è prevalsa storicamente la tendenza a dare forma di legge alle norme di protezione dei dati, il che ha consentito di sanzionare le violazioni e di riconoscere all'individuo il diritto ad un risarcimento. Tali leggi, inoltre, erano generalmente accompagnate da meccanismi procedurali supplementari, come la creazione di autorità di controllo con funzioni di vigilanza e di indagine in caso di denuncia. Questi aspetti procedurali sono ripresi nella direttiva 95/46/CE, con le sue disposizioni in materia di responsabilità, sanzioni, ricorsi, autorità di controllo e notifica-

zione. Al di fuori della Comunità è meno frequente imbattersi in simili strumenti procedurali, per garantire l'osservanza delle norme di tutela dei dati. Le parti che hanno sottoscritto la convenzione n. 108 devono dare forma di legge ai principi di protezione dei dati, ma non hanno alcun obbligo quanto ai meccanismi supplementari (ad esempio un'autorità di controllo). Gli orientamenti dell'OCSE prevedono solo l'obbligo per la legislazione nazionale di «prendere in considerazione» gli orientamenti medesimi, senza quindi offrire alcun mezzo procedurale atto a garantire una efficace tutela dell'individuo. I successivi orientamenti dell'ONU, invece, contengono alcune disposizioni relative al controllo e alle sanzioni, il che traduce la diffusa consapevolezza a livello internazionale della necessità di dare un'adeguata applicazione alle norme di tutela dei dati.

In questo contesto, un'analisi compiuta del significato di «tutela adeguata» deve tener conto di due elementi essenziali: il contenuto delle norme applicabili e gli strumenti per assicurarne un'efficace applicazione.

Prendendo come punto di partenza la direttiva 95/46/CE e tenendo presenti le disposizioni di altri testi normativi internazionali sulla protezione dei dati, dovrebbe essere possibile individuare un nucleo di principi di «contenuto» e di prescrizioni di «procedura/applicazione», la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della tutela. Si tratterebbe di una lista di riferimento duttile: eventualmente da integrare in alcuni casi, da ridimensionare quanto alle prescrizioni di altri. Il grado di rischio insito nel trasferimento per la persona interessata sarà un elemento importante ai fini della determinazione delle prescrizioni esatte di un caso particolare. Pur con questa limitazione, la compilazione di una lista di condizioni minime costituisce un utile punto di partenza per qualsiasi analisi.

(i) Principi di contenuto

I principi fondamentali da includere sono i seguenti:

1) il principio della finalità limitata: i dati dovrebbero essere trattati per una finalità specifica e successivamente utilizzati o ulteriormente comunicati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trasferimento. Le sole deroghe a tale norma sarebbero quelle necessarie in ogni società democratica per una delle ragioni elencate nell'articolo 13 della direttiva.⁵⁹⁾

2) il principio della qualità e della proporzionalità: i dati dovrebbero essere precisi e, se del caso, aggiornati. Essi dovrebbero essere adeguati, pertinenti e commisurati alle finalità per cui sono oggetto di trasferimento o di ulteriore trattamento.

⁵⁹⁾ L'articolo 13 prevede la possibilità di limitare il «principio della finalità, qualora tale restrizione costituisca una misura necessaria alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario, della protezione della persona interessata o dei diritti e delle libertà altrui».

3) **il principio della trasparenza:** la persona dovrebbe ricevere informazioni riguardanti la finalità del trattamento e l'identità del responsabile del trattamento nel paese terzo, nonché qualunque altra informazione necessaria ad assicurare una procedura equa. Le sole deroghe consentite dovrebbero essere in linea con l'articolo 11, paragrafo 2⁶⁰⁾ e con l'articolo 13 della direttiva.

4) **il principio della sicurezza:** il responsabile del trattamento dei dati dovrebbe adottare misure di sicurezza tecniche e organizzative commisurate ai rischi che il trattamento presenta. Chiunque operi sotto l'autorità del responsabile del trattamento, compresi gli incaricati del trattamento, procede al trattamento dei dati solo su istruzione del responsabile.

5) **i diritti di accesso, rettifica e opposizione:** la persona interessata dovrebbe avere diritto di ottenere una copia di tutti i dati trattati che la riguardano, nonché il diritto di far rettificare i dati di comprovata inesattezza. In determinate situazioni, la persona interessata dovrebbe inoltre potersi opporre al trattamento di dati che la riguardano. Le sole deroghe a tali diritti dovrebbero essere in linea con l'articolo 13 della direttiva.

6) **restrizioni ai successivi trasferimenti** di dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentite soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme che assicurano un livello adeguato di tutela. Le sole deroghe consentite dovrebbero essere in linea con l'articolo 26, paragrafo (1) della direttiva. Tali deroghe sono esaminate nel capitolo 5e.

Di seguito sono riportati alcuni esempi di principi supplementari da applicare in casi specifici di trattamento.

1) **dati sensibili:** se il trattamento riguarda categorie di dati «sensibili» (quelle elencate all'articolo 8 della direttiva⁶¹⁾), si dovrebbero porre in essere misure di salvaguardia supplementari, come ad esempio l'obbligo del consenso esplicito al trattamento da parte della persona interessata.

2) **commercializzazione diretta:** se il trasferimento dei dati avviene per finalità di commercializzazione diretta, la persona interessata dovrebbe essere in grado di decidere in qualsiasi momento l'esclusione dei dati che la riguardano da un simile impiego.

3) **decisioni individuali automatizzate:** se la finalità del trasferimento consiste nell'adozione di una decisione automatizzata ai sensi dell'articolo 15 della direttiva, la persona dovrebbe avere il diritto di conoscere la logica a cui tale decisione risponde e dovrebbero essere adottati altri provvedimenti per garantire la salvaguardia del suo interesse legittimo.

(ii) Meccanismi di procedura/applicazione

Vi è in Europa un ampio consenso circa la necessità di dare forma di legge ai principi di tutela dei dati. Ugualmente riconosciuta è la necessità di un sistema di «controllo esterno» sotto forma di autorità indipendente, atto ad assicurare

⁶⁰⁾ L'articolo 11, paragrafo (2) prevede che, nel caso in cui i dati non siano raccolti presso la persona interessata, a quest'ultima non debbano essere fornite informazioni quando ciò si rivela impossibile o richiede sforzi sproporzionati o la registrazione o la comunicazione è prescritta per legge.

⁶¹⁾ Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati relativi alla salute e alla vita sessuale e dati relativi a infrazioni, condanne penali o misure di sicurezza.

l'osservanza delle norme di tutela. Non in tutti i paesi, tuttavia, questi elementi sono presenti. Per fornire una base per la valutazione dell'adeguatezza della tutela offerta, è necessario individuare gli obiettivi di fondo di un sistema procedurale per la tutela dei dati e da qui procedere ad esaminare i diversi meccanismi procedurali giudiziari e non giudiziari applicati nei paesi terzi.

Gli obiettivi di un sistema di tutela dei dati sono essenzialmente tre:

1) assicurare un **buon livello di osservanza** delle norme (nessun sistema è in grado di garantire un'osservanza del 100%, ma alcuni sono migliori di altri). In un buon sistema, tra i responsabili del trattamento dei dati si può generalmente rilevare un elevato grado di consapevolezza dei propri obblighi e tra le persone interessate la medesima consapevolezza dei propri diritti e degli strumenti per esercitarli. Di particolare importanza, al fine di garantire il rispetto delle norme, è l'esistenza di sanzioni efficaci e dissuasive, al pari, ovviamente, di sistemi di verifica diretta da parte di autorità, revisori o addetti indipendenti alla tutela dei dati.

2) fornire **aiuto e sostegno alla persona interessata** nell'esercizio dei propri diritti. Ogni persona deve essere in grado di far rispettare i propri diritti in modo rapido ed efficace, ad un costo non proibitivo. A tal fine occorre porre in essere qualche meccanismo istituzionale che consenta di condurre un'indagine indipendente in caso di denuncia.

3) garantire un **risarcimento adeguato** alla parte lesa in caso di violazione delle norme. Si tratta di un elemento essenziale, che necessita di un sistema di arbitrato indipendente in grado di deliberare la corresponsione di un indennizzo e di imporre eventualmente sanzioni.

2. APPLICAZIONE DEI PRINCIPI AI PAESI CHE HANNO RATIFICATO LA CONVENZIONE N. 108 DEL CONSIGLIO D'EUROPA

Nel settore della protezione dei dati la convenzione n. 108 è l'unico strumento di diritto internazionale esistente oltre alla direttiva. La maggioranza dei firmatari è costituita da Stati membri dell'Unione europea (tutti i 15 hanno ormai ratificato la convenzione) o da paesi, come la Norvegia e l'Islanda, comunque vincolati dalla direttiva in forza dell'accordo sullo spazio economico europeo. Anche la Slovenia, l'Ungheria e la Svizzera hanno ratificato la convenzione e probabilmente altri paesi terzi lo faranno in futuro, tenuto conto in particolare del fatto che possono aderire alla convenzione anche paesi non membri del Consiglio d'Europa. Va quindi ben al di là di un interesse puramente accademico verificare se i paesi che hanno ratificato la convenzione si possono considerare in grado di garantire una tutela adeguata ai sensi dell'articolo 25 della direttiva.

Come punto di partenza è opportuno analizzare il testo della convenzione stessa alla luce del profilo teorico della «tutela adeguata» definito nel capitolo uno del presente documento.

Per quanto riguarda il contenuto dei principi di base, si può affermare che la convenzione soddisfa le prime cinque delle sei «condizioni minime»⁶²⁾. La convenzione prevede inoltre, a garanzia dell'adeguatezza della tutela dei dati particolarmente «sensibili», l'obbligo di adottare misure di salvaguardia appropriate.

⁶²⁾ Qualche dubbio può sussistere circa il «principio di trasparenza». L'articolo 8, lettera (a) della convenzione potrebbe non essere equivalente all'obbligo attivo di fornire informazioni, sancito dagli articoli 10 e 11 della direttiva. Inoltre, la convenzione non prevede in modo specifico il diritto di esclusione nel caso in cui i dati siano utilizzati a fini di commercializzazione diretta né contiene disposizioni circa le decisioni individuali automatizzate.

Per quanto riguarda il contenuto delle norme sostanziali della convenzione, una carenza è rappresentata dall'assenza di restrizioni al trasferimento verso paesi non firmatari. Questo comporta il rischio che un paese aderente alla convenzione sia utilizzato come «tappa intermedia» in un trasferimento di dati dalla Comunità verso un altro paese terzo in cui il livello di tutela è del tutto inadeguato.

Il secondo aspetto della «tutela adeguata» riguarda i meccanismi procedurali atti a garantire un'applicazione efficace dei principi di base. La convenzione impone ai paesi firmatari l'obbligo di dare forma di legge nazionale ai principi in essa contenuti e di istituire un sistema appropriato di sanzioni e di ricorsi in caso di violazione di detti principi. Ciò dovrebbe bastare ad assicurare un livello ragionevole di osservanza delle norme e un risarcimento adeguato della persona interessata in caso di inadempienza (obiettivi (1) e (3) di un sistema di tutela dei dati). La convenzione, tuttavia, non impone alle parti contraenti di creare meccanismi istituzionali che permettano di condurre indagini indipendenti in caso di denuncia, anche se in pratica è quanto hanno fatto in genere i paesi firmatari. Si tratta di una lacuna della convenzione, dal momento che l'assenza di tali meccanismi istituzionali non consente di garantire alla singola persona interessata un sostegno adeguato nell'esercizio dei propri diritti (obiettivo 2).

Questa breve analisi sembra indicare che, nella maggioranza dei casi, i trasferimenti di dati personali verso paesi che hanno ratificato la convenzione n. 108 si possono ritenere ammissibili ai sensi dell'articolo 25, paragrafo (1) della direttiva, a condizione che:

- il paese in questione disponga di meccanismi istituzionali appropriati che garantiscano l'osservanza delle norme e consentano di prestare assistenza alle persone interessate e assicurarne il risarcimento (come ad esempio un'autorità di controllo indipendente dotata di potere adeguati);

- il paese in questione sia destinatario finale del trasferimento e non una tappa intermedia attraverso cui i dati transitano, tranne il caso in cui i trasferimenti successivi siano diretti verso i paesi dell'Ue o verso un'altra destinazione che garantisca una tutela adeguata⁶³⁾.

Ovviamente questo esame della convenzione è abbastanza semplificato e superficiale. Casi specifici di trasferimenti di dati verso paesi firmatari della convenzione possono sollevare altri problemi che qui non sono stati presi in considerazione.

3. APPLICAZIONE DEI PRINCIPI ALL'AUTODISCIPLINA SETTORIALE

1. Introduzione

L'articolo 25, paragrafo 2, della direttiva sulla tutela dei dati personali (95/46/CE) statuisce che il livello di protezione garantito da un paese terzo deve essere valutato con riguardo a *tutte le circostanze* relative ad un trasferimento o ad una categoria di trasferimenti di dati. Si citano specificamente non solo le norme di diritto, ma anche «le regole professionali e le misure di sicurezza ivi osservate».

⁶³⁾ La convenzione n.108 è attualmente oggetto di una revisione, che potrebbe dar luogo a modifiche introdotte per superare queste e altre difficoltà.

Il testo della direttiva impone quindi di tenere conto delle norme di carattere non giuridico che possono essere in vigore nel paese terzo in questione, a patto che dette norme *siano rispettate*. È in questo contesto che va inquadrata la funzione dell'autodisciplina settoriale.

2. Che cos'è l'autodisciplina?

Il termine «autodisciplina» può assumere diversi significati. Nel presente documento per codice (o altro strumento) di autodisciplina s'intende qualsiasi complesso di norme per la tutela dei dati applicabili all'insieme dei responsabili del trattamento dei dati, appartenenti alla medesima professione od operanti nel medesimo settore economico, il cui contenuto è stato determinato essenzialmente da chi opera in tale settore o da chi esercita tale professione.

Si tratta di una definizione generale in cui può rientrare un'ampia gamma di strumenti, dal codice volontario di tutela dei dati elaborato dalla piccola associazione settoriale con solo pochi aderenti, fino al codice più articolato che fissa norme d'etica professionale applicabili a un'intera categoria professionale, ad es. medici o bancari, avente effetti pressoché analoghi a quelli giurisdizionali.

3. L'organismo responsabile del codice è rappresentativo del settore?

Come si chiarirà in questo capitolo, un importante parametro del valore di un codice è il grado di applicazione delle sue disposizioni. In questo contesto, la questione della rappresentatività dell'associazione o dell'organismo responsabile del codice, ossia se essi rappresentino tutti gli operatori del settore o solo una piccola percentuale di essi, è probabilmente meno importante rispetto alla determinazione del potere dell'associazione in termini di capacità, ad esempio, di applicare sanzioni agli aderenti che non rispettano il codice. Tuttavia, per varie altre ragioni, i codici applicabili a un intero settore o a un'intera professione, e aventi un campo d'applicazione definito in modo chiaro e dettagliato, sono degli strumenti di tutela più utili dei codici sviluppati da piccoli raggruppamenti di aziende all'interno dei vari settori. Anzitutto, dal punto di vista del consumatore, un settore non compatto e in cui operano molte associazioni rivali, ciascuna con un proprio codice di tutela dei dati, crea confusione. L'esistenza parallela di molti codici differenti crea un'immagine globale priva di trasparenza per la persona interessata. In secondo luogo, segnatamente per attività quali la vendita diretta, in cui è prassi corrente trasmettere i dati personali da una società all'altra, può succedere che la società che comunica i dati e la società ricevente non siano vincolate dal medesimo codice di tutela. Ciò è una fonte di incertezza circa la natura delle norme applicabili e può rendere più difficile l'esame dei reclami presentati dalle persone interessate e la ricerca di una soluzione.

4. Valutazione dell'autodisciplina: criteri da seguire

Vista la grande varietà di strumenti compresi nel termine autodisciplina, è palese la necessità di differenziare le varie forme di autodisciplina in base al loro reale effetto sul livello di tutela offerto quando i dati personali sono trasferiti in un paese terzo.

Per valutare qualsiasi corpo specifico di norme per la tutela dei dati (che rientri nella categoria dell'autodisciplina o in quella della regolamentazione) è necessario fare riferimento ai principi generali enunciati nel capitolo 1. È di fon-

damentale importanza non limitare l'esame dello strumento al suo contenuto (che dovrà abbracciare una serie di principi di base) ma estenderlo alla sua efficacia nel conseguire:

- un buon livello generale di osservanza
- sostegno e assistenza alle persone interessate dal trattamento dei dati,
- mezzi di riparazione adeguati (ivi incluso il risarcimento se necessario)

5. Valutazione del contenuto di uno strumento di autodisciplina

È un compito relativamente facile. Si tratta di accertare la presenza dei necessari «principi di contenuto» enumerati nel capitolo 1. Si tratta di una valutazione obiettiva, che verte sul contenuto del codice e non sulle modalità con cui è stato elaborato. Il fatto che un settore economico o una professione abbia avuto un ruolo chiave nell'elaborazione del contenuto del codice non è di per sé rilevante, benché sia evidente che se nella sua elaborazione si è tenuto conto del parere delle persone interessate e delle organizzazioni dei consumatori, è più probabile che esso rispecchi più rigorosamente i requisiti basilari di tutela dei dati. La trasparenza del codice è un elemento determinante; soprattutto, è necessario che il codice sia redatto in un linguaggio semplice e offra esempi concreti, che ne illustrino le disposizioni. Il codice dovrebbe inoltre vietare la comunicazione dei dati a società che non abbiano sottoscritto il codice e che pertanto non vi siano assoggettate, a meno che non siano offerte altre garanzie adeguate.

6. Valutazione dell'efficacia dello strumento di autodisciplina

Valutare l'efficacia di un determinato codice o strumento di autodisciplina è un compito più arduo, che richiede la comprensione dei dispositivi che garantiscono il rispetto del codice e con i quali si regolano i problemi inerenti alle violazioni. Perché un codice di autodisciplina possa essere considerato atto a garantire una tutela adeguata, è necessario che siano soddisfatti i tre criteri funzionali su cui si basa la valutazione dell'efficacia della tutela.

Buon livello di osservanza

I codici settoriali o professionali sono di norma elaborati da un organo rappresentativo del settore o della professione e si applicano agli aderenti della categoria che fa capo a tale organo rappresentativo. Il grado di osservanza del codice dipende verosimilmente dal fatto che i membri sappiano che esso esiste e ne conoscano il contenuto, dalle misure adottate per renderlo trasparente agli occhi dei consumatori, consentendo alle forze di mercato di dare un contributo concreto, dall'esistenza di un sistema di controllo esterno (quale ad esempio l'obbligo di accertamento periodico della sua osservanza) e, cosa forse più importante, dal genere di sanzioni contemplate in caso di violazione e dalla loro applicazione.

È perciò importante chiedersi:

- Che cosa fa l'organo rappresentativo per garantire la conoscenza del codice tra i suoi aderenti?
- L'organo rappresentativo esige che i suoi aderenti dimostrino di aver applicato concretamente le disposizioni contemplate dal codice? Con che frequenza?
- Tale prova è fornita dall'impresa aderente stessa o da una fonte esterna (quale ad esempio un revisore riconosciuto)?

– L'organo rappresentativo esamina le violazioni, denunciate o presunte, del codice?

– L'osservanza del codice è una condizione per l'adesione all'organo rappresentativo o l'osservanza è puramente «facoltativa»?

– Qualora sia dimostrato che un aderente abbia violato il codice, di quali sanzioni disciplinari (espulsione o altro) può valersi l'organo rappresentativo?

– In caso di provvedimento d'espulsione da parte dell'organo rappresentativo, la società o l'individuo possono continuare ad operare nello stesso settore o ad esercitare la stessa professione?

– Il rispetto del codice può essere imposto in altro modo, ad esempio per via giudiziaria o mediante un organo avente giurisdizioni speciali? In taluni paesi i codici professionali o deontologici sono legalmente vincolanti. In alcuni casi ci si può persino valere delle norme di legge relative alle pratiche commerciali leali o addirittura alla concorrenza per far applicare i codici settoriali.

Allorché si esaminano i tipi di sanzioni comminate, è importante distinguere tra sanzioni «correttive», che, in caso di inosservanza, si limitano a esigere che il responsabile del trattamento dei dati modifichi le proprie pratiche adeguandole alle disposizioni del codice, e le sanzioni che vanno oltre e puniscono il responsabile del trattamento dei dati per la sua inadempienza. Solo questa seconda categoria di sanzioni «punitive» incide realmente sulla futura condotta dei responsabili del trattamento dei dati, incentivandoli a rispettare il codice in modo regolare.

La mancanza di sanzioni realmente dissuasive e punitive è, per un codice, una grave debolezza. Senza tali sanzioni è difficile immaginare come si possa ottenere un buon grado di osservanza generale, a meno che non esista un rigoroso sistema di controllo esterno (ad esempio un'autorità pubblica o privata abilitata ad intervenire in caso di inosservanza del codice, o l'obbligo di sottoporsi a una verifica esterna periodica).

Sostegno e assistenza alle persone interessate dal trattamento dei dati

Un requisito fondamentale a garanzia dell'adeguatezza e dell'efficacia del sistema di tutela dei dati è rappresentato dal fatto che chiunque abbia un problema circa il trattamento di dati che lo riguardano non sia abbandonato a se stesso, ma goda del sostegno di una istanza prevista dal sistema di tutela medesimo, per poter risolvere il suo problema. Idealmente, questa istanza di sostegno dovrebbe essere imparziale, indipendente e dotata dei poteri necessari per indagare in merito a eventuali reclami sporti dalle persone interessate. Gli interrogativi riguardanti l'autodisciplina che si pongono sotto questo profilo sono i seguenti:

– Esiste un dispositivo che permetta di indagare in merito ai reclami presentati dalle singole persone interessate?

– Come sono informate le persone interessate dell'esistenza di detto dispositivo e delle decisioni prese nei singoli casi?

– Le persone interessate debbono sostenere dei costi?

– Chi conduce le indagini? Tale persona / organo dispone di sufficienti poteri al riguardo?

– Chi decide in merito ad un'asserita violazione del codice? Si tratta di persone indipendenti e imparziali?

L'imparzialità dell'arbitro o della persona investita della decisione in merito all'asserita violazione del codice è fondamentale. È ovvio che tale persona od organo debbano essere indipendenti dal responsabile del trattamento dei dati.

Tuttavia questo in sé non basta a garantire l'imparzialità. Idealmente l'arbitro dovrebbe essere estraneo alla professione o al settore in questione, poiché chi esercita la stessa professione od opera nel medesimo settore ha chiaramente interessi comuni al responsabile del trattamento dei dati accusato di violazione del codice. Se così non è, la neutralità dell'organo investito della decisione può essere garantita mediante l'inclusione (in pari numero) di rappresentanti dei consumatori e di rappresentanti del settore.

Riparazione adeguata

Qualora si dimostri che il codice di autodisciplina è stato violato, la persona interessata dovrebbe avere la possibilità di ottenere riparazione. Tale riparazione deve ovviare al problema (ad es. rettificare o eliminare i dati erranei, porre fine al trattamento dei dati per fini incompatibili) e, qualora la persona interessata abbia subito dei danni, deve permettere un adeguato risarcimento pecuniario. Va ricordato che il termine «danno» ai sensi della direttiva concernente la tutela di dati non indica unicamente i danni materiali e finanziari, ma anche i danni psicologici e morali (noti come «distress» nel diritto del Regno Unito e degli Stati Uniti).

Molti dei quesiti relativi alle sanzioni, riportati nella sezione precedente intitolata «Buon livello di osservanza», sono pertinenti anche in questo contesto. Come precedentemente detto, le sanzioni hanno una duplice funzione: punire chi commette l'infrazione (stimolando quindi il trasgressore e gli altri aderenti a rispettare le norme) e rimediare alla violazione delle norme. È principalmente questa seconda funzione che prendiamo qui in considerazione. Ulteriori interrogativi potrebbero perciò essere:

- È possibile verificare se un aderente, a carico del quale è stata accertata una violazione del codice, ha modificato le sue pratiche e rimediato al problema?

- Le persone interessate possono ottenere un risarcimento in base al codice, e come?

- La violazione del codice è equiparabile all'inadempienza contrattuale, o regolata dal diritto comune (ad es. tutela dei consumatori, concorrenza sleale), e possono le autorità giudiziarie competenti accordare il risarcimento dei danni su tale base?

7. Conclusioni

- L'autodisciplina dovrebbe essere valutata in base ai criteri obiettivi e funzionali enunciati nel capitolo 1.

- Uno strumento di autodisciplina può essere considerato un valido elemento di «adeguata tutela» solo se è vincolante per tutti coloro che vi sono assoggettati, a cui sono trasferiti i dati personali, e se offre sufficienti garanzie qualora i dati siano trasmessi a terzi non aderenti.

- Lo strumento deve essere trasparente e incorporare nella sostanza i principi basilari relativi alla tutela dei dati.

- Lo strumento deve avere dispositivi che assicurino effettivamente un buon livello di osservanza generale. Un sistema di sanzioni dissuasive e punitive è una delle possibilità a tale fine. Un'altra sono i controlli esterni obbligatori.

- Lo strumento deve offrire sostegno e assistenza alle persone interessate che abbiano un problema relativo al trattamento dei loro dati personali. È pertanto necessario istituire un organismo indipendente, imparziale e facilmente accessibile che esamini i reclami presentati dalle persone interessate e decida in merito alle violazioni del codice.

– Lo strumento deve garantire un'adeguata riparazione in caso di inosservanza. La persona interessata deve poter ottenere un provvedimento di riparazione e se del caso un risarcimento.

4. IL RUOLO DELLE DISPOSIZIONI CONTRATTUALI

1. Introduzione

In base al principio stabilito all'articolo 25, paragrafo 1 della direttiva relativa alla protezione dei dati (95/46/CE), il trasferimento di dati personali verso paesi terzi può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato. In questo capitolo sono esaminate le possibili deroghe al principio della «tutela adeguata» dell'articolo 25 previste dall'articolo 26, paragrafo 2. Tale disposizione permette a uno Stato membro di autorizzare un trasferimento o una categoria di trasferimenti verso un paese terzo «non adeguato» «qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi». La disposizione in seguito specifica che «tali garanzie possono segnatamente risultare da clausole contrattuali». Ai sensi dell'articolo 26, paragrafo 4 la Commissione può inoltre, secondo la procedura di cui all'articolo 31, decidere che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui all'articolo 26, paragrafo 2.

L'idea di ricorrere a contratti come mezzo per regolamentare i trasferimenti internazionali di dati personali non è stata ovviamente introdotta dalla direttiva. Già nel 1992 il Consiglio d'Europa, la Camera di commercio internazionale e la Commissione europea avevano effettuato congiuntamente uno studio in merito⁶⁴⁾. In tempi più recenti un numero crescente di esperti e di commentatori, forse notando l'esplicito riferimento nella direttiva, hanno formulato in studi e articoli osservazioni circa l'utilizzazione di contratti. Questi ultimi hanno continuato ad essere utilizzati nel «mondo reale» come mezzo per ovviare ai problemi inerenti alla protezione dei dati derivanti dal trasferimento di dati personali da alcuni Stati membri dell'Ue. I contratti sono stati largamente utilizzati in Francia a partire dalla fine degli anni «'80, mentre in Germania il recente caso della «Bahncard» che ha coinvolto la Citibank è stato oggetto di notevole pubblicità⁶⁵⁾.

2. Utilizzazione di contratti come base per i trasferimenti intracomunitari di dati

Prima di esaminare i requisiti delle disposizioni contrattuali nel contesto dei flussi di dati verso paesi terzi, occorre chiarire la differenza tra la situazione in un paese terzo e quella esistente all'interno della Comunità. In quest'ultimo caso, il contratto rappresenta il meccanismo utilizzato per definire e regolamentare la ripartizione delle responsabilità in materia di protezione dei dati ove più di un soggetto sia interessato al trattamento dei dati in questione. Ai sensi della

⁶⁴⁾ «Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum», studio effettuato congiuntamente dal Consiglio d'Europa, dalla Commissione delle Comunità europee e dalla Camera di commercio internazionale, Strasburgo, 2 novembre 1992.

⁶⁵⁾ Cfr. la presentazione di Alexander Dix del caso in questione in occasione dell'«International Data Protection and Privacy Commissioners» Conference», settembre 1996, Ottawa.

direttiva un soggetto, il «responsabile del trattamento», deve assumere la responsabilità principale dell'osservanza dei principi essenziali di protezione dei dati. Il secondo soggetto, l'«incaricato del trattamento», è responsabile unicamente della sicurezza dei dati. Per responsabile del trattamento si intende un soggetto dotato di poteri di decisione circa le finalità e le modalità di trattamento dei dati, mentre l'incaricato del trattamento è unicamente il soggetto che fornisce fisicamente il servizio di trattamento dei dati. La relazione tra i due soggetti è definita all'articolo 17, paragrafo 3 della direttiva:

– *l'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:*

– *che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;*

– *che gli obblighi di cui al paragrafo 1 (disposizioni essenziali riguardo alla sicurezza dei dati), quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.*

Ciò deriva dal principio generale di cui all'articolo 16, in base al quale l'incaricato del trattamento o chiunque agisca sotto l'autorità del responsabile del trattamento non deve elaborare dati personali, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi di legge.

Anche nel caso di trasferimento di dati personali verso paesi terzi, in genere sarà coinvolta più di una parte. In questo caso la relazione è tra il soggetto che trasferisce i dati (il «cedente») e il soggetto che riceve i dati nel paese terzo (il «destinatario»). In questo contesto uno degli obiettivi del contratto dovrebbe essere quello di determinare le modalità di ripartizione della responsabilità in materia di protezione dei dati tra le due parti. Il contratto deve però mirare anche ad altro, cioè a fornire garanzie supplementari alla persona interessata dal trattamento dei dati, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto a un complesso di norme vincolanti in materia di protezione dei dati, atte a garantire un livello adeguato di tutela.

3. Obiettivo di una soluzione contrattuale

Nell'ambito del trasferimento verso paesi terzi, quindi, il contratto costituisce un mezzo per il responsabile del trattamento di fornire garanzie adeguate al momento di trasferire i dati al di fuori della Comunità (e quindi al di fuori della tutela prevista dalla direttiva, nonché dal contesto generale della legislazione comunitaria⁶⁶⁾) verso un paese terzo in cui il livello generale di protezione non sia adeguato. Per soddisfare tale funzione, una disposizione contrattuale deve compensare in modo soddisfacente la mancanza di un livello generale di protezione adeguata e comportare gli elementi essenziali di tutela che possono mancare in una qualsiasi situazione particolare.

⁶⁶⁾ L'esercizio dei diritti in materia di tutela dei dati personali è facilitato nell'ambito della Comunità dal contesto giuridico generale, ad esempio dall'accordo di Strasburgo (1977) sulla trasmissione di richieste di assistenza giuridica.

4. Requisiti specifici di una soluzione contrattuale

Il punto di partenza per valutare il significato delle «garanzie sufficienti» di cui all'articolo 26, paragrafo 2, è la nozione di «tutela adeguata», già esaminata nel capitolo 1, nel quale sono stati individuati alcuni principi fondamentali in materia di protezione dei dati e talune condizioni necessarie per assicurarne l'efficacia.

(i) Norme fondamentali in materia di protezione dei dati

Il primo requisito della soluzione contrattuale è, quindi, che le parti interessate al trasferimento dei dati siano obbligate a garantire l'applicazione dei principi fondamentali in materia di protezione dei dati enunciati nel capitolo 1 al trattamento dei dati trasferiti verso il paese terzo. Tali principi fondamentali sono:

- il principio della finalità limitata
- il principio della qualità e della proporzionalità
- il principio della trasparenza
- il principio della sicurezza
- i diritti di accesso, rettifica e opposizione
- restrizioni ai successivi trasferimenti verso parti non firmatarie del contratto⁶⁷⁾.

Inoltre, in alcune situazioni vanno applicati altri principi relativi ai dati sensibili, alla commercializzazione diretta e alle decisioni automatizzate.

Nel contratto andrebbe precisato in che modo il destinatario del trasferimento dei dati dovrà applicare tali principi (ad esempio, andrebbero specificate le finalità, le categorie di dati, i termini di conservazione, le misure di sicurezza, ecc.). In altre situazioni, ad esempio quando in un paese terzo la protezione dei dati è garantita da norme analoghe a quelle previste dalla direttiva, è probabile che esistano altri meccanismi che precisano le modalità di applicazione pratica delle norme di protezione dei dati (codici di comportamento, notificazione, funzione di consulenza dell'autorità di controllo). In una situazione contrattuale ciò non avviene ed è quindi indispensabile, quando il trasferimento avviene in base a un contratto, specificare i dettagli.

(ii) Rendere efficaci le norme fondamentali

Nel capitolo 1 sono enunciati tre criteri in base ai quali andrebbe valutata l'efficacia del sistema di protezione dei dati. Tali criteri si riferiscono alla capacità del sistema di:

- assicurare un **buon livello di osservanza** delle norme;
- fornire **sostegno e assistenza alle persone interessate dal trattamento dei dati** nell'esercizio dei propri diritti;
- elemento di importanza essenziale, garantire una **riparazione adeguata** alla parte lesa in caso di inosservanza delle norme.

Nel valutare l'efficacia di una soluzione contrattuale vanno applicati gli stessi criteri. Si tratta evidentemente di una sfida difficile ma non impossibile. Occorre trovare un mezzo che possa compensare l'assenza di meccanismi di

⁶⁷⁾ Non dovrebbero essere autorizzati ulteriori trasferimenti dei dati personali dal destinatario a terzi, a meno che non si trovi il modo di obbligare contrattualmente questi ultimi a fornire alle persone interessate le stesse garanzie di tutela dei dati.

controllo e di imposizione e fornire sostegno, assistenza e, in ultima analisi, una riparazione adeguata alla persona interessata, anche se non firmataria del contratto.

Ognuno di questi aspetti va esaminato nei dettagli. Per facilitare l'analisi, essi vengono esaminati in ordine inverso.

Garantire una riparazione alla persona interessata

Garantire alla persona interessata la possibilità di un ricorso legale (ossia il diritto di presentare un reclamo ad un arbitro indipendente che possa giudicare in merito e di ottenere, se del caso, una riparazione) tramite un contratto tra il «cedente» e il «destinatario» dei dati non è una questione semplice. Molto dipenderà dalla natura della legislazione in materia di contratti prescelta come legge nazionale applicabile al contratto. Prevedibilmente la legge applicabile sarà in genere quella dello Stato membro in cui la parte cedente è stabilita. In alcuni Stati membri la legislazione in materia di contratti consente l'istituzione di diritti di terzi, che invece non è possibile in altri Stati membri.

In genere, comunque, quanto più il destinatario è limitato per quanto riguarda la possibilità di scegliere le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, tanto maggiore è la sicurezza giuridica per la persona interessata. Tenendo presente che si sta trattando di casi di protezione generale inadeguata, la soluzione migliore sarebbe quella di specificare nel contratto che il destinatario del trasferimento in questione non ha alcun potere autonomo di decisione per quanto riguarda i dati trasferiti o il modo in cui essi vengono trattati successivamente. Il destinatario è tenuto ad agire soltanto dietro istruzioni del cedente e, anche nel caso in cui i dati siano stati fisicamente trasferiti al di fuori dell'Ue, il controllo decisionale sui dati spetta sempre al soggetto, stabilito nella Comunità, che ha effettuato il trasferimento. In tal modo il cedente resta il responsabile del trattamento, mentre il destinatario è semplicemente un subcontraente incaricato del trattamento. In questo caso, dato che il controllo dei dati è esercitato da un soggetto stabilito in uno Stato membro dell'Ue, la legislazione dello Stato membro in questione continuerà ad essere applicabile al trattamento effettuato nel paese terzo⁶⁸⁾ e inoltre il responsabile del trattamento continuerà, ai sensi della legislazione di tale Stato membro, ad essere responsabile di eventuali danni cagionati da un trattamento illecito⁶⁹⁾.

Disposizioni di questo tipo non sono dissimili da quelle previste dall'«Accordo inter-territoriale» che ha risolto il caso Citibank «Bahncard» menzionato in precedenza. In questo caso, l'accordo contrattuale fissava nei dettagli le disposizioni riguardanti il trattamento dei dati, in particolare quelle relative alla sicurezza dei dati, e ne vietava qualsiasi altra utilizzazione da parte del destina-

⁶⁸⁾ Ai sensi dell'art. 4, paragrafo 1, lettera a), della direttiva 95/46/CE.

⁶⁹⁾ Cfr. art. 23 della direttiva 95/46/CE.

tario del trasferimento. Nell'accordo la legislazione tedesca veniva applicata al trattamento dei dati effettuato nel paese terzo, garantendo in tal modo un ricorso legale alle persone interessate⁷⁰⁾.

Naturalmente in certi casi sarà impossibile ricorrere a questa soluzione. Potrebbe darsi che il destinatario del trasferimento non debba semplicemente fornire un servizio di trattamento dei dati al responsabile del trattamento stabilito nell'Ue, ma abbia, ad esempio, noleggiato o acquistato i dati per utilizzarli per i propri interessi o i propri scopi. In tali circostanze il destinatario dovrà disporre di una certa libertà nel trattamento dei dati, diventando in pratica a tutti gli effetti un «responsabile del trattamento» dei dati.

In casi del genere non è possibile fare affidamento sull'applicabilità automatica permanente della legislazione di uno Stato membro e sulla responsabilità permanente del cedente per eventuali danni causati. Per fornire alle persone interessate un adeguato ricorso legale vanno concepiti altri meccanismi più complessi. Come si è detto in precedenza, alcuni ordinamenti giuridici consentono a terzi la rivendicazione di diritti in forza di un contratto e questa possibilità potrebbe essere utilizzata per istituire i diritti delle persone interessate grazie ad un contratto pubblico e pubblicato tra il cedente e il destinatario. La posizione delle persone interessate verrebbe ulteriormente rafforzata qualora, nell'ambito del contratto, le parti si impegnassero a sottoporsi ad una specie di arbitrato vincolante nel caso in cui una persona interessata dal trattamento dei dati contestasse un'inadempienza. Alcuni codici di autodisciplina settoriale includono tali meccanismi di arbitrato, e potrebbe essere utile prevedere l'utilizzazione di contratti abbinata a tali codici.

Un'altra possibilità consiste nello stipulare, eventualmente al momento dell'ottenimento iniziale dei dati, un accordo contrattuale separato tra il cedente e la persona interessata dal trattamento dei dati, in base al quale il cedente mantiene la responsabilità di eventuali danni o difficoltà causate dall'inosservanza, da parte del destinatario del trasferimento dei dati, dei principi fondamentali concordati in materia di protezione dei dati. In questo modo la persona interessata ha la garanzia di un ricorso contro il cedente per le infrazioni del destinatario. Spetterebbe allora al cedente ottenere il risarcimento dei danni pagati alla persona interessata, intentando causa al destinatario per inadempienza contrattuale.

Una soluzione a tre così complessa è forse più attuabile di quanto sembri a prima vista. Il contratto con la persona interessata potrebbe diventare parte integrante delle condizioni generali tipo in base alle quali una banca o un'agenzia di viaggi, ad esempio, fornisce servizi ai clienti, presentando inoltre il vantaggio della trasparenza: la persona interessata è perfettamente a conoscenza dei suoi diritti.

⁷⁰⁾ Peraltro, dato che il caso è sopravvenuto nell'ambito di una legislazione precedente alla direttiva, la legislazione stessa non è stata applicata automaticamente a tutti i trattamenti controllati da un responsabile del trattamento insediato in Germania. Il ricorso legale per le persone interessate è stato invece possibile grazie alla legislazione contrattuale tedesca che consente di istituire diritti di terzi.

Infine, come alternativa a un contratto con la persona interessata, si potrebbe prospettare la possibilità, per uno Stato membro, di disporre per legge una responsabilità permanente dei responsabili del trattamento che trasferiscono dati al di fuori della Comunità per quanto riguarda eventuali danni causati dalle azioni del destinatario del trasferimento.

Fornire sostegno e assistenza alle persone interessate dal trattamento dei dati

Una delle principali difficoltà cui devono far fronte le persone i cui dati vengono trasferiti verso una giurisdizione straniera è l'incapacità di scoprire la causa originaria del problema particolare che le affligge, da cui consegue l'impossibilità di giudicare se le norme di protezione dei dati siano state correttamente osservate oppure se sussistano motivi di ricorso legale ⁷¹⁾. Per un livello di tutela adeguato è quindi necessario un qualche meccanismo istituzionale che permetta indagini indipendenti in caso di reclamo.

Le funzioni di vigilanza e di investigazione esercitate dall'autorità di controllo di uno Stato membro si limitano al trattamento dei dati effettuato nel territorio dello Stato membro in questione ⁷²⁾. Quando i dati vengono trasferiti verso un altro Stato membro, un sistema di assistenza reciproca tra le autorità di controllo garantisce che un eventuale reclamo di una persona interessata nel primo Stato membro venga sottoposto ad un'indagine adeguata. Quando invece il trasferimento è effettuato verso un paese terzo, nella maggior parte dei casi tale garanzia non esiste. Si tratta quindi di esaminare che tipo di meccanismo di compensazione possa essere adottato nel contesto di un trasferimento di dati sulla base di un contratto.

Una possibilità sarebbe quella di esigere semplicemente una clausola contrattuale che garantisca all'autorità di controllo dello Stato membro in cui è stabilito il cedente il diritto di controllare il trattamento effettuato dall'incaricato del trattamento nel paese terzo. Nella pratica, tale controllo potrebbe essere effettuato da un agente (ad esempio, una società di certificazione specializzata) designato dall'autorità di controllo, ove necessario. Una difficoltà inerente a un metodo del genere, tuttavia, consiste nel fatto che l'autorità di controllo in genere ⁷³⁾ non è parte del contratto e, di conseguenza, in alcune giurisdizioni potrebbe non avere i mezzi di appellarsi ad esso per avere accesso. Un'altra possibilità sarebbe un impegno legale assunto dal destinatario nel paese terzo direttamente nei confronti dell'autorità di controllo dello Stato membro dell'Ue interessato, in base al quale il destinatario dei dati autorizza l'accesso all'autorità di controllo o a un agente designato qualora insorgano sospetti di inosservanza dei principi in materia di protezione dei dati. In virtù di tale impegno, le parti interessate dal trasferimento dei dati potrebbero anche informare l'autorità di controllo circa qualsiasi reclamo ricevuto dalle persone interessate dal trattamento dei dati. In questo caso tale impegno sarebbe una condizione preliminare per l'autorizzazione al trasferimento dei dati.

⁷¹⁾ Anche se i diritti delle persone interessate sono stati garantiti nell'ambito di un contratto, tali persone spesso non saranno in grado di giudicare se si sia verificata un'inadempienza contrattuale e da parte di chi. È quindi necessaria una procedura investigativa al di fuori delle procedure legali del diritto civile ufficiale.

⁷²⁾ Cfr. art. 28, paragrafo 1, della direttiva 95/46/CE.

⁷³⁾ Secondo la delegazione francese potrebbero verificarsi situazioni in cui l'autorità di controllo è parte firmataria del contratto.

Indipendentemente dalla soluzione prescelta, resta assai dubbio se sia opportuno, pratico o semplicemente fattibile, dal punto di vista delle risorse, che un'autorità di controllo di uno Stato membro dell'Ue assuma la responsabilità di esaminare e controllare il trattamento di dati effettuato in un paese terzo.

Garantire un buon livello di osservanza

Anche in mancanza di un particolare reclamo o di difficoltà riscontrate da una persona interessata dal trattamento dei dati, è indispensabile un elevato grado di fiducia nell'osservanza delle condizioni contrattuali da parte dei firmatari. Il problema della soluzione contrattuale consiste nella difficoltà di stabilire, in caso di inadempienza del contratto, sanzioni che siano sufficientemente significative per ottenere l'effetto dissuasivo necessario per garantire tale fiducia. Anche qualora un controllo efficace dei dati continuasse ad essere esercitato dall'interno della Comunità, il destinatario del trasferimento potrebbe non incorrere in alcuna sanzione penale diretta, anche se il trattamento dei dati avvenisse in violazione del contratto. La responsabilità incomberebbe invece al cedente stabilito nella Comunità, che dovrebbe poi ottenere il risarcimento di eventuali danni intentando una causa a parte contro il destinatario. Una responsabilità indiretta del genere potrebbe non essere sufficiente a indurre il destinatario all'osservanza di tutti i dettagli del contratto.

Stando così le cose, è probabile che nella maggior parte dei casi una soluzione contrattuale dovrà essere integrata quanto meno dalla possibilità di una qualche forma di controllo esterno delle attività di trattamento del destinatario, ad esempio una verifica effettuata da un ente di normalizzazione o da una società di certificazione specializzata.

5. Il problema della legge prevalente

Una difficoltà propria del metodo contrattuale è la possibilità che la legislazione generale del paese terzo contempli l'obbligo, per il destinatario del trasferimento dei dati, di rivelare - in determinati casi - dati personali alle autorità pubbliche (polizia, tribunali o fisco, ad esempio) e che tali obblighi legali prevalgano su qualsiasi contratto che l'incaricato del trattamento abbia sottoscritto⁷⁴⁾. Per gli incaricati del trattamento all'interno della Comunità questa possibilità è prevista dall'articolo 16 della direttiva, secondo cui l'incaricato del trattamento può elaborare i dati solo dietro istruzione del responsabile del trattamento oppure *in virtù di obblighi legali*. Ai sensi della direttiva, peraltro, la rivelazione di informazioni (che sia per sua natura per finalità incompatibili con quelle per le quali i dati sono stati raccolti) va limitata al minimo necessario in società democratiche e per uno dei motivi di «ordine pubblico» di cui all'articolo 13, paragrafo 1 della direttiva. Anche l'articolo 6 del trattato di Amsterdam garantisce il rispetto dei diritti fondamentali stabiliti nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Nei paesi terzi non sempre esistono per i poteri pubblici analoghe limitazioni all'ottenimento di dati personali da società e da altre organizzazioni operanti sul loro territorio.

⁷⁴⁾ La portata dei poteri pubblici per quanto concerne l'obbligo di rivelare informazioni è un aspetto di cui tener conto anche al momento di una valutazione più generale dell'adeguatezza della tutela in un paese terzo.

Non è facile venire a capo di questa difficoltà, che dimostra chiaramente i limiti del metodo contrattuale. In alcuni casi il contratto è uno strumento troppo fragile per offrire garanzie adeguate di protezione dei dati, e non andrebbero autorizzati trasferimenti verso certi paesi.

6. Considerazioni pratiche in merito sull'uso dei contratti

Dall'analisi precedente si è visto che qualsiasi soluzione contrattuale deve essere definita in modo dettagliato e opportunamente adatta al trasferimento di dati in questione. Questa necessità di precisare le finalità e le condizioni di trattamento dei dati trasferiti non esclude la possibilità di elaborare un modello di contratto tipo che però, per ogni contratto, andrà completato in modo da adattarlo alle circostanze particolari del caso.

L'analisi ha inoltre dimostrato che esistono difficoltà pratiche particolari nell'esame dei casi di inadempienza di un contratto quando il trattamento avviene al di fuori dell'Ue e quando nel paese terzo in questione non esiste alcuna forma di autorità di controllo. Questo significa che in alcune situazioni la soluzione contrattuale potrà essere quella appropriata, mentre in altre il contratto non potrà garantire la necessaria tutela adeguata.

La necessità di adattare in modo particolareggiato il contratto alle peculiarità del trasferimento in questione implica che un contratto è particolarmente adatto a situazioni in cui i trasferimenti di dati sono simili e di natura ripetitiva. Date le difficoltà inerenti al controllo, una soluzione contrattuale può essere maggiormente efficace quando le parti del contratto sono operatori importanti già sottoposti a controllo e regolamentazione pubblica⁷⁵⁾. Le grandi reti internazionali, ad esempio quelle utilizzate per le transazioni nel campo delle carte di credito e per le prenotazioni aeree, presentano entrambe queste caratteristiche; sono queste le situazioni in cui i contratti possono rivelarsi più utili. In queste circostanze possono anche essere integrati da convenzioni multilaterali intese a fornire una migliore sicurezza giuridica. Allo stesso modo, quando le parti interessate dal trasferimento sono affiliate o fanno parte dello stesso gruppo di imprese, la capacità di indagare in merito sull'inadempienza di un contratto è presumibilmente molto rafforzata, dati gli stretti legami tra il destinatario nel paese terzo e il soggetto stabilito nella Comunità. I trasferimenti all'interno di una stessa impresa sono quindi un altro settore in cui il ricorso a soluzioni contrattuali può rivelarsi particolarmente efficace.

Conclusioni e raccomandazioni principali

– Nell'ambito della Comunità i contratti vengono utilizzati come mezzo per stabilire la ripartizione delle responsabilità in materia di osservanza della protezione dei dati tra il responsabile del trattamento e il subcontraente incaricato del trattamento. Quando ha luogo un trasferimento di dati verso paesi, il contratto deve fornire alle persone interessate dal trattamento dei dati garanzie supplementari, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto in materia di protezione dei dati a norme vincolanti atte a fornire un livello di tutela adeguato.

⁷⁵⁾ Nel caso Citibank «Bahncard» il sovrintendente alla tutela dei dati di Berlino ha cooperato con le autorità di controllo bancario americane.

– La base per la valutazione dell'adeguatezza delle garanzie fornite da una soluzione contrattuale è la stessa che per la valutazione del livello generale di adeguatezza in un paese terzo. Una soluzione contrattuale deve comprendere tutti i principi fondamentali in materia di protezione dei dati e fornire mezzi con cui rendere applicabili tali principi.

– Nel contratto andrebbero specificati in dettaglio le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, nonché le modalità di applicazione dei principi fondamentali in materia di protezione dei dati. Una maggiore sicurezza giuridica è offerta da contratti in cui viene limitata la libertà del destinatario dei dati di trattare questi ultimi in modo autonomo per proprio conto. Il contratto andrebbe quindi utilizzato, nei limiti del possibile, come mezzo con cui il soggetto che trasferisce i dati mantiene il controllo decisionale sul trattamento effettuato nel paese terzo.

– Se il destinatario dispone di un certo grado di autonomia nel trattamento dei dati trasferiti, la situazione è più complessa e non sempre un solo contratto tra le parti interessate al trasferimento può costituire una base sufficiente per l'esercizio dei diritti da parte delle persone interessate dal trattamento dei dati. Può essere necessario un meccanismo in forza del quale la parte stabilita nella Comunità che provvede al trasferimento resta responsabile di eventuali danni causati dal trattamento effettuato nel paese terzo.

– I trasferimenti successivi verso enti od organizzazioni non vincolate dal contratto andrebbero esplicitamente esclusi dal contratto in questione, a meno che non sia possibile vincolare per contratto tali terzi a rispettare gli stessi principi in materia di protezione dei dati.

– Il grado di fiducia nel rispetto dei principi in materia di protezione dei dati dopo il trasferimento dei dati stessi verrebbe rafforzato se l'osservanza dei principi di protezione dei dati da parte del destinatario del trasferimento fosse sottoposta ad una verifica esterna da parte, ad esempio, di una società di certificazione specializzata o di un istituto di normalizzazione.

– Nel caso in cui una persona interessata dal trattamento dei dati subisca le conseguenze di una violazione delle disposizioni in materia di protezione dei dati previste dal contratto, il problema generale è quello di garantire che il reclamo della persona interessata venga adeguatamente esaminato. Le autorità di controllo degli Stati membri dell'Ue incontreranno difficoltà pratiche nel procedere a tale esame.

– Le soluzioni contrattuali sono probabilmente più adatte alle grandi reti internazionali (carte di credito, prenotazioni aeree) caratterizzate da grandi quantità di trasferimenti di dati ripetitivi di natura simile e da un numero relativamente esiguo di importanti operatori in settori già sottoposti ad un elevato grado di controllo e di regolamentazione pubblica. I trasferimenti tra le filiali di uno stesso gruppo costituiscono un altro campo che si presta in modo particolare all'utilizzazione dei contratti.

– I paesi in cui le autorità pubbliche dispongono in materia di accesso alle informazioni di poteri più estesi di quelli ammessi dalle norme internazionalmente riconosciute in materia di tutela dei diritti dell'uomo non sono da considerarsi destinazioni sicure per i trasferimenti basati su clausole contrattuali.

5. DEROGHE AL PRINCIPIO DELL'ADEGUATEZZA

L'articolo 26, paragrafo 1 della direttiva prevede, per un numero limitato di situazioni, la possibilità di derogare al principio della «adeguatezza» per i trasferimenti in paesi terzi. Queste deroghe, che sono descritte dettagliatamente, riguardano soprattutto casi in cui i rischi per l'interessato sono ridotti o in cui altri interessi (interessi pubblici o quelli della persona stessa cui i dati si riferiscono) prevalgono sul diritto dell'interessato alla riservatezza. In quanto deroghe a un principio generale, devono essere interpretate in modo restrittivo. Inoltre, nella legislazione nazionale gli Stati membri possono stabilire che le deroghe non si applicano in determinati casi. Ciò può succedere, ad esempio, quando è necessario tutelare gruppi di individui particolarmente vulnerabili, come i lavoratori o i pazienti.

La prima di queste deroghe comprende i casi in cui l'interessato dà in modo *inequivocabile* il proprio consenso al trasferimento proposto. Un punto importante da tenere presente è che il consenso, secondo la definizione dell'articolo 2, lettera *h*) della direttiva, va dato liberamente, in maniera specifica e informata. L'obbligo d'informazione è particolarmente importante dato che prescrive che l'interessato sia informato adeguatamente sul rischio specifico che i suoi dati vengano trasferiti in un paese che non garantisce una tutela adeguata. Se non viene data quest'informazione, la deroga non si applica. Poiché il consenso dev'essere inequivocabile, anche il dubbio sul fatto che esso sia stato dato rende la deroga inapplicabile. Ciò potrebbe significare che molte situazioni in cui il consenso è implicito (ad esempio perché un individuo è stato informato su un trasferimento e non si è opposto) non giustificano questa deroga. Tuttavia, la deroga potrebbe essere utile nei casi in cui chi effettua il trasferimento ha un contatto diretto con la persona interessata e in cui le informazioni necessarie possono essere fornite facilmente e il consenso ottenuto in modo inequivocabile. Questo avviene spesso nel caso di trasferimenti effettuati quando, ad esempio, si stipula un'assicurazione.

La seconda e la terza deroga riguardano i trasferimenti *necessari* per l'esecuzione di un contratto fra l'interessato e il responsabile del trattamento (o l'applicazione delle misure precontrattuali prese su richiesta dell'interessato) oppure per la conclusione o l'esecuzione di un contratto concluso *nell'interesse della persona interessata* tra il responsabile del trattamento e un terzo. Potenzialmente, queste deroghe appaiono abbastanza ampie, ma in pratica, come per la quarta e quinta deroga esaminate più avanti, la loro applicazione può essere limitata dalla «test di necessità»: tutti i dati trasferiti devono essere necessari per l'esecuzione del contratto. Quindi, se vengono trasferiti dati supplementari non essenziali o se il trasferimento non è finalizzato all'esecuzione del contratto, bensì ad altri obiettivi (ad esempio la successiva commercializzazione) la deroga non si applica. Per quanto riguarda le situazioni precontrattuali, queste comprenderebbero soltanto situazioni poste in essere per iniziativa dell'interessato (come la richiesta di informazioni su un determinato servizio) e non quelle risultanti da approcci di commercializzazione effettuati dal responsabile del trattamento.

Nonostante queste restrizioni, la seconda e terza deroga non rimarranno senza conseguenze. È probabile che saranno applicate frequentemente, ad esempio, ai trasferimenti necessari per prenotare un biglietto aereo per un passeggero, per le operazioni di una banca internazionale o per i pagamenti mediante carta di credito. La deroga per i contratti «nell'interesse della persona

interessata» (articolo 26, paragrafo 1, lettera c) comprende infatti in particolare il trasferimento di dati sui beneficiari di pagamenti bancari, che, sebbene interessati, spesso non sono parte di un contratto con il responsabile del trattamento che effettua il trasferimento.

La quarta deroga ha due elementi costitutivi. Il primo comprende i trasferimenti necessari o prescritti dalla legge per la salvaguardia di un interesse pubblico rilevante in base a importanti motivi di interesse pubblico. Si può trattare di trasferimenti limitati fra le amministrazioni pubbliche, ma occorre fare attenzione a non interpretare questa disposizione in modo troppo ampio. Il semplice interesse pubblico non basta a giustificare un trasferimento, è necessario che sia una questione di interesse pubblico *rilevante*. Il considerando 58 indica che saranno compresi in generale i trasferimenti di dati fra le amministrazioni fiscali o doganali o fra i servizi responsabili della sicurezza sociale. Anche i trasferimenti fra gli organi di controllo nel settore dei servizi finanziari possono beneficiare della deroga. Il secondo elemento costitutivo riguarda i trasferimenti che avvengono nell'ambito di controversie internazionali o di procedimenti giudiziari, in particolare i trasferimenti necessari per costatare, esercitare o difendere un diritto per via giudiziaria.

La quinta deroga riguarda i trasferimenti necessari per la salvaguardia degli interessi vitali della persona interessata. Ad esempio, potrebbe trattarsi del trasferimento urgente di documenti medici a un paese terzo, dove un turista che ha usufruito precedentemente di cure mediche nell'Ue, ha subito un incidente o si è ammalato gravemente. Occorre tenere presente, tuttavia, che il considerando 31 della direttiva dà una definizione di «interesse vitale» abbastanza limitata, nel senso che dev'essere un interesse «essenziale alla vita della persona interessata». Questo escluderebbe normalmente, per esempio, gli interessi finanziari, patrimoniali o familiari.

La sesta ed ultima deroga riguarda i trasferimenti effettuati a partire da registri destinati per legge alla consultazione da parte del pubblico, purché siano rispettate nel caso specifico le condizioni previste per la consultazione. La ragione di questa deroga è che se in uno Stato membro un registro può essere consultato pubblicamente o dalle persone che dimostrano un interesse legittimo, il fatto che la persona autorizzata a consultare il registro si trovi in un paese terzo e che la consultazione richieda di fatto un trasferimento di dati non deve impedire che l'informazione gli sia trasmessa. Il considerando 58 precisa che questa deroga non permette il trasferimento della totalità dei dati o delle categorie di dati contenuti nel registro. In ragione di tali restrizioni, questa deroga non dev'essere considerata una deroga generale per il trasferimento di dati dei registri pubblici. Chiaramente, essa non intende permettere il trasferimento massiccio di dati dei registri pubblici per scopi commerciali o l'utilizzo di dati disponibili pubblicamente per individuare persone con un profilo specifico.

6. QUESTIONI PROCEDURALI

L'articolo 25 dispone che la valutazione dell'adeguatezza avvenga caso per caso, in relazione ai singoli trasferimenti o alle singole categorie di trasferimenti. Tuttavia, considerati l'elevato numero di trasferimenti di dati personali in uscita dalla Comunità ogni giorno e la molteplicità delle parti interessate da tali trasferimenti, è evidente che nessuno Stato membro, qualunque sia il sistema

adottato per l'applicazione dell'articolo 25 ⁷⁶⁾, sarà in grado di garantire che ogni singolo caso sia esaminato in dettaglio. Ovviamente ciò non significa che nessun caso sarà esaminato in dettaglio, ma indica piuttosto la necessità di elaborare meccanismi volti a razionalizzare il processo decisionale per un gran numero di casi e a consentire l'adozione di decisioni, almeno a carattere provvisorio, senza ritardi inutili e senza dispendio eccessivo di risorse.

Tale razionalizzazione si impone a prescindere da chi decide, che si tratti di un responsabile del trattamento dei dati, dell'autorità di controllo o di un altro organismo istituito secondo le procedure vigenti nello Stato membro.

(i) Ricorso all'articolo 25, paragrafo 6 della direttiva

Un modo ovvio di contribuire a questa razionalizzazione, previsto nella direttiva stessa, consisterebbe nel determinare che certi paesi terzi assicurano un adeguato livello di tutela. Tali constatazioni avrebbero un valore «puramente indicativo» e quindi non si applicherebbero a casi presentanti difficoltà particolari. Tuttavia, questa sarebbe una soluzione pratica del problema. Queste indicazioni permetterebbero in particolare agli operatori economici di sapere quali paesi assicurano in generale un livello «adeguato» di tutela e costituirebbero un incentivo chiaro e pubblico per i paesi terzi che stanno sviluppando o migliorando i loro sistemi di tutela. Una serie di indicazioni a livello comunitario contribuirebbe inoltre ad affrontare in modo coerente questa questione ed eviterebbe il proliferare di «liste bianche» diverse ed eventualmente in conflitto fra loro, stabilite dai governi degli Stati membri o dalle autorità di tutela dei dati.

Comunque, questo approccio non è privo di difficoltà, la principale delle quali è che molti paesi terzi non garantiscono una tutela uniforme in tutti i settori economici. Molti paesi sono dotati ad esempio di una normativa sulla tutela dei dati nel settore pubblico ma non in quello privato. In alcuni paesi, per esempio negli Stati Uniti, esistono norme specifiche solo per particolari settori (per es. le informazioni sulla solvibilità e gli archivi per il noleggio video nel caso degli USA). Un'ulteriore difficoltà deriva dallo statuto federale di alcuni paesi come gli USA, il Canada e l'Australia, dove le norme sono spesso diverse da uno Stato all'altro della federazione. Ne risulta che attualmente molti paesi terzi non possono essere considerati in grado di offrire una tutela globale adeguata. Se il numero di paesi per i quali possono essere date indicazioni positive è esiguo, diminuisce naturalmente anche l'utilità dell'esercizio, nel senso che dà minore certezza ai responsabili del trattamento. Un altro rischio è che alcuni paesi terzi possano interpretare la mancanza di una constatazione come una provocazione politica o una discriminazione, poiché tale mancanza potrebbe essere una conseguenza sia del fatto che il loro caso non è stato esaminato sia di un giudizio sul loro sistema di tutela dei dati.

Dopo aver considerato attentamente questi diversi argomenti, il gruppo di lavoro è tuttavia dell'opinione che sarebbe utile avviare i lavori necessari per procedere alle constatazioni previste dall'articolo 25, paragrafo 6. Dovrebbe trattarsi di un processo permanente, che darebbe modo di stabilire un elenco di paesi non definitivo, ma costantemente aggiornato e riveduto alla luce dei

⁷⁶⁾ Gli Stati membri possono istituire procedure amministrative diverse per l'adempimento degli obblighi previsti dall'articolo 25: per esempio, possono imporre un obbligo diretto al responsabile del trattamento dei dati e/o mettere a punto un sistema di autorizzazione preventiva o di verifica retroattiva del parte dell'autorità di controllo.

nuovi sviluppi. Una constatazione positiva non dovrebbe, in linea di principio, limitarsi ai paesi in cui esistono leggi orizzontali sulla tutela dei dati, ma dovrebbe riguardare anche specifici settori di un paese per i quali la tutela dei dati è adeguata, anche se in altri settori dello stesso paese la tutela dovesse risultare inadeguata.

Occorre osservare che il gruppo istituito dall'articolo 29 non ha funzioni decisionali esplicite in merito a particolari trasferimenti di dati o alla determinazione dell'«adeguatezza» ai sensi all'articolo 25, paragrafo 6. In entrambi i casi si applica la procedura del comitato di cui all'articolo 31. Va comunque notato che uno dei compiti specifici del gruppo consiste nel fornire alla Commissione un parere sul livello di tutela nei paesi terzi (vedi articolo 30, paragrafo 1, lettera b). Rientra quindi tra i compiti del gruppo esaminare la situazione in determinati paesi terzi e formulare un parere provvisorio sull'adeguatezza della tutela. Le constatazioni positive, una volta confermate a norma dell'articolo 25, paragrafo 6, per essere utili dovrebbero essere ampiamente diffuse. Nel caso in cui si sia constatato che un paese non assicura una tutela adeguata, ciò non dovrà significare l'iscrizione di tale paese, implicita o esplicita, in una «lista nera». Il messaggio pubblico sarà piuttosto l'impossibilità di fornire per il momento un'indicazione generale riguardo a quel particolare paese.

(ii) Analisi dei rischi relativi a trasferimenti specifici

Sebbene il ricorso all'articolo 25, paragrafo 6 analizzato sopra possa facilitare notevolmente le decisioni relative a molti casi di trasferimento di dati, resteranno comunque numerosi i casi in cui il paese terzo in questione non è oggetto (globalmente o parzialmente) di un parere favorevole. Il trattamento che gli Stati membri riservano a casi del genere può variare a seconda delle modalità di recepimento dell'articolo 25 nella normativa nazionale (cfr. la precedente nota a piè di pagina). Se all'autorità di controllo è attribuita una competenza specifica per l'autorizzazione preventiva dei trasferimenti dei dati ovvero per l'esecuzione di una verifica retroattiva, l'elevato volume di trasferimenti in gioco renderà necessario un sistema che consenta di stabilire un calendario di priorità per le attività di detto organismo. Tale sistema potrebbe consistere in una serie concordata di criteri che permettano di determinare se un trasferimento o una categoria di trasferimenti siano da considerarsi prioritari in quanto rappresentino una particolare minaccia per la vita privata delle persone interessate.

Un sistema del genere non comporterebbe alcuna modifica dell'obbligo per ciascuno Stato membro di autorizzare soltanto i trasferimenti verso paesi terzi con un adeguato grado di protezione. Esso sarebbe d'aiuto per stabilire quali casi di trasferimenti di dati debbano essere esaminati o anche investigati in via «prioritaria» e permetterebbe di dirigere le risorse disponibili verso quei trasferimenti che sollevano le maggiori preoccupazioni in materia di protezione della persona interessata.

Il gruppo ritiene che fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione siano comprese le seguenti:

- trasferimenti riguardanti le categorie particolari di dati di cui all'articolo 8 della direttiva;
- trasferimenti che comportano rischi di perdite finanziarie (ad esempio pagamenti con carta di credito attraverso Internet);
- trasferimenti che comportano rischi per la sicurezza personale;

- trasferimenti finalizzati all'adozione di una decisione particolarmente importante per la persona interessata (assunzioni, promozioni, concessione di un credito, ecc.);
- trasferimenti che rischiano di causare un grave imbarazzo a una persona o di lederne la reputazione;
- trasferimenti che possono condurre ad azioni specifiche che costituiscono un'ingerenza grave nella vita privata della persona (per esempio, telefonate indesiderate);
- trasferimenti ripetuti che riguardano grandi volumi di dati (per es. dati su transazioni elaborati su reti di telecomunicazioni, Internet, ecc.);
- trasferimenti che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti «cookies» di Internet).

(i) Clausole contrattuali tipo

Come è stato discusso ampiamente nel capitolo 4, la direttiva prevede la possibilità che anche nel caso in cui il livello di tutela non sia adeguato, il responsabile del trattamento possa ottenere una protezione adeguata del trasferimento dei dati mediante un contratto. L'articolo 26, paragrafo 2 della direttiva permette agli Stati membri di autorizzare trasferimenti in base a disposizioni contrattuali, una decisione che deve essere notificata in seguito alla Commissione. Se esistono opposizioni all'autorizzazione, la decisione può essere respinta o confermata dalla Commissione conformemente alla procedura del comitato di cui all'articolo 31. Oltre alle autorizzazioni concesse dagli Stati membri, l'articolo 26, paragrafo 4 della direttiva permette anche alla Commissione, sempre in conformità alla procedura del comitato di cui all'articolo 31, di decidere se certe clausole contrattuali tipo offrono garanzie sufficienti. Tali decisioni sono vincolanti per gli Stati membri.

Data l'evidente complessità e difficoltà di queste soluzioni contrattuali, è necessario che i responsabili del trattamento che intendono utilizzare i contratti in questo modo possano avvalersi di un orientamento. A livello degli Stati membri, spetterà alle autorità nazionali competenti la responsabilità principale di questo orientamento, particolarmente per quanto riguarda la preparazione delle autorizzazioni nell'ambito dell'articolo 26, paragrafo 2. Le autorità degli Stati membri e la Commissione dovrebbero cooperare e scambiare opinioni sulle clausole contrattuali loro presentate.

Quando le clausole tipo proposte vengono presentate alle autorità degli Stati membri o direttamente alla Commissione, dovrebbe essere adottata una procedura che consenta l'esame delle clausole anche da parte del gruppo, per evitare differenze nello sviluppo delle pratiche nazionali e per far sì che la Commissione possa usufruire della consulenza specialistica appropriata prima di prendere qualsiasi decisione ai sensi dell'articolo 26, paragrafo (4).

ALLEGATO 1

**CONSEGUENZE PRATICHE DEGLI ARTICOLI 25 E 26 DELLA DIRETTIVA
SUL TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI**

INTRODUZIONE

La questione del trasferimento verso paesi terzi è affrontata in questo documento secondo un approccio globale comprendente:

- una valutazione della tutela adeguata ai sensi dell'articolo 25 della direttiva sulla tutela dei dati;

- una valutazione dei mezzi alternativi per garantire una protezione adeguata tramite soluzioni contrattuali, come previsto dall'articolo 26, paragrafo 2;
- una valutazione delle deroghe al principio della tutela adeguata previste dall'articolo 26, paragrafo 1.

La problematica non sarebbe trattata in modo esauriente se non si esaminassero le conseguenze pratiche di questo approccio globale per i trasferimenti di dati personali. Nel presente allegato, perciò, alcuni casi realistici, ma fittizi, di trasferimenti di dati sono esaminati secondo il metodo che dovrebbe essere adottato quando saranno entrate in vigore le leggi nazionali d'attuazione della direttiva.

Vengono presentati tre casi diversi, per ognuno dei quali si valuta dapprima se la tutela nel paese destinatario è adeguatamente assicurata da leggi pertinenti o da un'efficace autodisciplina del settore privato. In caso negativo, si procede alla ricerca di una soluzione del problema nell'ambito delle possibilità previste dall'articolo 26, paragrafi 1 (deroghe) e 2 (soluzioni contrattuali). Soltanto in mancanza di una soluzione appropriata si passerà al blocco del trasferimento.

CASO (1): UN TRASFERIMENTO DI DATI RIGUARDANTI LA CAPACITÀ DI CREDITO

Un cittadino della Comunità desidera comprare una casa per le vacanze in un paese A al di fuori della CE e chiede un prestito ad un'istituzione finanziaria di quel paese. Questa si rivolge ad un'agenzia d'informazioni commerciali per ottenere informazioni sulla solvibilità del cliente. L'agenzia non ha un dossier su questa persona, ma dispone che un suo curriculum finanziario completo sia trasferito dall'agenzia affiliata del Regno Unito. Il paese A è un paese altamente industrializzato, con istituzioni democratiche antiche e stabili. Il suo sistema giudiziario è ben organizzato ed efficiente. Ha una struttura costituzionale federale.

FASE 1: VALUTAZIONE DELL'ADEGUATEZZA DELLA TUTELA

Le norme applicabili pertinenti

Il responsabile del trattamento destinatario è soggetto alla legge federale che stabilisce norme sulle informazioni personali detenute per la valutazione dei rischi di credito. Il responsabile del trattamento s'impegna inoltre ad attenersi alla propria politica della privacy resa pubblica. Non è applicabile alcuna legge statale e non esiste un codice di autodisciplina settoriale.

Valutazione del contenuto delle norme applicabili

Innanzitutto va notato che la comunicazione effettuata dall'agenzia di informazioni commerciali situata nel Regno Unito sarebbe soggetta, come qualsiasi comunicazione a un responsabile del trattamento nel Regno Unito o in un altro Stato membro, agli obblighi previsti dalla legislazione del Regno Unito, che attua tutti gli articoli della direttiva fuorché gli articoli 25 e 26. Questo è importante perché evita la necessità di esaminare la legalità della comunicazione stessa e permette di concentrare l'attenzione sulla tutela di cui godranno i dati una volta trasferiti nel paese A.

La valutazione del contenuto delle norme dovrebbe, logicamente, iniziare dalla legislazione federale. In caso di lacune, si potrebbe considerare se la normativa meno «rigida» in materia di «privacy» permette di colmarle. Diamo qui

di seguito un elenco dei contenuti che si possono ritenere necessari e un giudizio circa la presenza di questo contenuto necessario nella legislazione o nella politica della privacy.

Il principio della finalità limitata, in questo contesto, può riguardare soltanto l'obbligo che tutti gli usi secondari e la comunicazione dei dati trasferiti siano compatibili con la finalità per cui sono stati trasferiti. L'inclusione dei dati in una «mailing list» destinata alla vendita o al noleggio sul mercato dev'essere considerata incompatibile, come anche la comunicazione dei dati a possibili datori di lavoro o a partner d'affari interessati alla solvenza della persona interessata. La comunicazione dei dati ad altri prestatori (banche, società di carte di credito) può comunque essere considerata compatibile.

In questo caso la legge federale stabilisce un numero limitato di finalità per le quali le informazioni commerciali personali possono essere comunicate legittimamente. Queste finalità comprendono «l'impiego» e «le legittime esigenze connesse ad un'operazione commerciale in cui la persona interviene». In questo concetto sono comprese anche talune utilizzazioni di dati a fini commerciali, tra cui la commercializzazione di beni o servizi diversi dal credito da parte di terzi. La legge federale non sembra quindi limitare sufficientemente la finalità e su questo punto la tutela non è adeguata. La politica della società in fatto di privacy non migliora la situazione.

Il principio della trasparenza dovrebbe comportare che l'interessato sia informato sull'identità dell'agenzia d'informazione commerciale del paese A e su ogni altra finalità del trattamento dei dati. Il modo esatto in cui questo avviene dovrebbe essere comparabile a quello stabilito nell'articolo 11 della direttiva. In questo caso la legge federale non contiene disposizioni specifiche sulla trasparenza che riguardino direttamente l'agenzia d'informazioni commerciali. Tuttavia, il prestatore del paese A è tenuto a comunicare all'interessato che saranno richieste informazioni ad un'agenzia d'informazioni commerciali, anche se non sarà necessario fornire il nome e l'indirizzo dell'agenzia. La persona interessata non ha quindi alcuna garanzia legale di essere informata del fatto che l'agenzia d'informazioni commerciali in questione procede a un trattamento di dati che lo riguardano. Poiché l'agenzia non ha contatti diretti con l'interessato, l'obbligo di contattarlo appositamente per informarlo sembra costituire uno «sforzo sproporzionato» ai sensi dell'articolo 11 della direttiva. Il livello di tutela per quanto riguarda la trasparenza pare quindi sufficiente.

Il principio della qualità e della proporzionalità comprende diversi elementi. La legge federale non prevede restrizioni alla raccolta e al trattamento di dati non necessari. Per quanto riguarda la durata della loro conservazione, ci sono norme che vietano la diffusione di informazioni obsolete (dichiarazioni di fallimento anteriori a 10 anni), e ne comportano di fatto la cancellazione. Non vi è alcun obbligo legale generale di conservare i dati con accuratezza, ma se una persona chiede di accedere alle informazioni commerciali che lo riguardano e contesta alcune di esse, i dati che non possono essere verificati vanno cancellati. Anche in questi casi la tutela non pare totalmente adeguata e la politica di privacy della società non va al di là della legge federale.

Il principio della sicurezza si traduce nella legge federale nell'obbligo di adottare misure appropriate per impedire una comunicazione illegale. La politica di privacy della società avverte che vengono effettuati severi controlli per impedire l'accesso non autorizzato alle informazioni commerciali e la loro mani-

polazione. Questi controlli consistono in dispositivi tecnici (parole chiave, ecc.) e in istruzioni ai dipendenti, la cui inosservanza può dar luogo a procedimenti disciplinari. Ciò sembra assicurare un livello adeguato di sicurezza.

I diritti di accesso e rettifica sono garantiti dalla legge federale e sono comparabili a quelli previsti dalla direttiva. Nel caso in cui a una persona sia rifiutato un credito, l'accesso alle informazioni che la riguardano è gratuito. Non esiste, comunque, un **diritto di opposizione**, anche se la persona può presentare ricorso presso un'agenzia federale specializzata oppure intentare un'azione legale (vedi sotto) se sono stati violati diritti di cui gode in forza della legge federale.

I dati riservati sulla salute dell'individuo fanno parte dei dati trasferiti. La legge federale comprende disposizioni più severe riguardanti il trattamento dei dati relativi a precedenti penali, sesso, razza, origine etnica, età e stato civile, ma non allo stato di salute. La politica di privacy dell'agenzia d'informazioni commerciali prevede che i dati sulla salute non siano utilizzati al fine di valutare la capacità di credito, ma solo per controlli sull'impiego o sull'assicurazione. In questi due casi l'uso dei dati sarà autorizzato dall'interessato nella domanda di assunzione o nel modulo d'assicurazione. Sembrerebbe dunque che per i dati sulla salute considerati in quest'esempio la tutela sia notevolmente maggiore, anche se non garantita per legge.

È qui in questione anche l'utilizzazione di dati per fini di commercializzazione diretta da parte dell'agenzia di informazioni commerciali (e la comunicazione dei dati ad altri per tali fini). Non esiste alcuna disposizione di legge che vieti tale utilizzazione né alcun obbligo giuridico di dare alla persona interessata la possibilità di opporvisi. Questa situazione è chiaramente inadeguata, in particolare perché i dati possono essere utilizzati dall'agenzia (per costituire «mailing lists» da offrire a istituti di credito) ma anche comunicati a terzi per la commercializzazione di prodotti attinenti a servizi finanziari o anche senza alcun rapporto con essi (per es. falciatrici da giardino o vacanze).

Il fine del trasferimento sembra essere quello di permettere una **decisione automatizzata** circa la concessione o meno di un credito alla persona interessata. In questo contesto, essa dovrebbe quindi beneficiare di un'ulteriore tutela. Sebbene la legge federale comprenda disposizioni che permettono alla persona di contestare le informazioni fornite da un'agenzia e, se necessario, di aggiungergli spiegazioni, non esistono norme che permettono di impugnare una decisione presa in base ad informazioni errate o incomplete, di riesaminarla e, se l'impugnazione è giustificata, di cambiarla. Il meccanismo permette di modificare un rapporto in modo da evitare problemi futuri, ma non risolve necessariamente il problema di una decisione di credito già presa. Questa tutela giuridica non retroattiva è insufficiente.

Restrizioni ai trasferimenti ulteriori di dati verso un altro paese terzo o verso organizzazioni di altri settori del paese A non soggetti alle norme della legge federale. Disposizioni in questo senso non esistono né nella legge federale né nella politica di privacy della società.

Campo d'applicazione della legge federale e della politica di privacy. Sarebbe necessario un altro controllo per accertare che la legislazione e la politica di privacy si applicano ai dati riguardanti tutte le persone e non soltanto i residenti o i cittadini del paese A. In tal caso, non esistono restrizioni del campo d'applicazione.

Valutazione dell'efficacia della tutela

La normativa federale in questione ha forza di legge ed istituisce anche un'autorità pubblica con alcuni poteri di controllo esterno. Per far valere i loro diritti, le persone possono inoltre promuovere privatamente un'azione legale. Tuttavia, l'autorità pubblica non ha l'obbligo preciso d'indagare su ogni singolo reclamo e, secondo taluni commentatori, non è sempre stata particolarmente attiva nel far rispettare la legge. Le cause private sono un metodo costoso e spesso lento per chi vuol far valere i propri diritti, soprattutto se vive in un paese diverso da quello in cui ha luogo il processo.

La politica di privacy interna della società non comprende un meccanismo indipendente che permetta alla persona di far valere i propri diritti, ma prevede sanzioni disciplinari per i dipendenti che non rispettano tale politica. Alcuni dipendenti hanno già subito provvedimenti disciplinari per passate violazioni.

La combinazione di legislazione e codice interno di privacy va valutata in base agli «obiettivi» che sono stati fissati per i meccanismi procedurali. Gli aspetti fondamentali a questo riguardo sono:

Un buon livello d'osservanza generale

Il miglior incentivo perché una società rispetti la propria politica di privacy è il rischio di pubblicità negativa sui giornali nel caso in cui non mantenesse le sue promesse. Inoltre, i dipendenti della società possono subire misure disciplinari se non si attengono alle regole di sicurezza.

Questi meccanismi non sembrano comunque sufficienti ad assicurare che la politica di privacy sia rispettata nella pratica.

La conclusione sarebbe stata diversa se:

1) la politica di privacy della società avesse rispecchiato un codice di condotta stabilito dall'associazione di categoria e valido per l'intero settore, che preveda l'immediata esclusione dall'associazione delle società che non rispettano tale codice; oppure

2) una norma di legge generale permettesse ad un organo pubblico di perseguire per pratiche «sleali ed ingannevoli» una società che non rispetta il proprio codice di privacy reso pubblico.

La legge federale incoraggia il rispetto delle norme in quanto prevede la possibilità di promuovere azioni legali private in caso di inosservanza. La prospettiva di finire in tribunale può avere un effetto deterrente sul responsabile del trattamento dei dati. Tuttavia, il controllo esterno diretto delle procedure di trattamento dei dati è molto limitato, dato che le autorità pubbliche reagiscono soltanto se un problema viene portato alla loro attenzione, ad esempio da un querelante o dalla stampa.

Sostegno ed aiuto alle persone interessate

Esiste un'agenzia pubblica a cui le persone possono rivolgersi per presentare i loro reclami circa le informazioni commerciali che li riguardano. L'esame del reclamo non comporta alcun costo per l'interessato.

Risarcimento adeguato

In caso di violazione degli obblighi previsti dalla legge federale, la persona può ottenere un risarcimento dal tribunale. Si tratta comunque di un processo relativamente costoso e spesso l'interessato non riceve in queste procedure il sostegno dell'agenzia pubblica. Il tribunale può imporre al responsabile del trattamento di risarcire gli eventuali danni, nonché di correggere le sue procedure di

trattamento dei dati ed il contenuto del dossier commerciale in questione. Non è invece possibile una riparazione in caso di inosservanza dei principi di tutela dei dati previsti soltanto dalla politica di privacy.

Il giudizio

1) Alcuni principi di tutela dei dati, definiti «principi fondamentali» nel documento di discussione, sono contenuti in certa misura nella legge federale applicabile alle informazioni commerciali. Altri si trovano invece nella politica di privacy. Anche considerando gli uni e gli altri, non si può dire, però, che tutti i «principi fondamentali» siano presenti; alcuni di essi (per es. il principio della finalità limitata) lo sono in forma assai blanda

2) Un problema più generale è se la politica di privacy di una società possa essere considerata in ogni caso un meccanismo abbastanza efficace. A meno che un'associazione di categoria o un organismo pubblico possa esercitare poteri di controllo esterno che ne permettono un'effettiva applicazione, tale politica risulta in larga misura inapplicabile e non può quindi essere presa in considerazione.

3) Sebbene l'organismo pubblico istituito per applicare la legge federale non abbia gli stessi poteri di un tipico organo europeo per la protezione dei dati, la legge garantisce una certa sicurezza giuridica, particolarmente nell'ambito di un sistema giudiziario efficiente e della «cultura processuale» esistente nel paese A. La legge contiene chiare disposizioni sul principio di protezione dei dati forse più importante di tutti, il diritto di accesso e di rettifica, e alcune limitazioni dei fini per i quali i dati possono essere utilizzati.

Conclusione

La tutela risulta inadeguata perché la legge include un numero insufficiente di «principi fondamentali» e la politica di privacy, di per sé, non è un mezzo di tutela efficace. Un giudizio di adeguatezza presupporrebbe che nella legge fossero inclusi principi come la trasparenza e la protezione dei dati sulla salute oppure che la politica di privacy fosse resa più efficace grazie a uno dei metodi suggeriti sopra (ossia fare del rispetto del codice di condotta una condizione per poter essere membro di un'associazione di categoria oppure dare a un organo pubblico il potere di ricorrere in giudizio contro la società per pratiche sleali e ingannevoli).

FASE 2: RICERCA DI UNA SOLUZIONE

Delle possibili deroghe indicate nell'articolo 26, paragrafo 1, soltanto la (a), il consenso della persona interessata, appare adeguata. La deroga (b), che riguarda i trasferimenti necessari per l'esecuzione di un contratto, non è applicabile perché la parte cedente, l'agenzia di informazioni commerciali situata nel Regno Unito, non ha un rapporto contrattuale con l'interessato. È difficile anche sostenere che il trasferimento sia necessario per la conclusione di un contratto «nell'interesse della persona interessata» come richiesto per la deroga (c).

Il consenso dell'interessato sembrerebbe essere una soluzione relativamente semplice del problema. Il consenso potrebbe essere ottenuto direttamente dall'agenzia situata nel Regno Unito oppure per conto dell'agenzia britannica dall'istituzione finanziaria del paese A, che potrebbe chiedere il consenso sul

modulo di domanda del credito. Qualsiasi metodo venga scelto, l'individuo dovrebbe essere informato del rischio particolare risultante dal fatto che i suoi dati devono essere trasferiti verso un paese che non garantisce una tutela adeguata.

Dato che questo tipo di trasferimento è ancora relativamente insolito, l'ottenimento del consenso di volta in volta è probabilmente la soluzione più pratica. Se le agenzie di informazioni commerciali di tutto il mondo inizieranno a scambiarsi dati in modo più sistematico, potranno essere trovate altre vie, come soluzioni contrattuali o un codice internazionale di condotta.

CASO (2): IL TRASFERIMENTO DI DATI RISERVATI NELL'INDUSTRIA AEREA

Un cittadino portoghese prenota un biglietto di volo di una compagnia aerea del paese B presso un'agenzia di viaggi di Lisbona. I dati raccolti contengono informazioni sul fatto che il cittadino è disabile e fa uso di una sedia a rotelle. Essi sono immessi in un sistema di prenotazione computerizzato internazionale e da qui sono trasferiti nella base di dati sui passeggeri della compagnia aerea situata nel paese B, dove vengono conservati fino a data indeterminata. La compagnia aerea intende utilizzare i dati per fornire un servizio migliore al passeggero se in futuro viaggerà ancora sui suoi voli, oltre che per scopi di programmazione della gestione interna ⁷⁷⁾.

FASE 1: VALUTAZIONE DELL'ADEGUATEZZA DELLA TUTELA

Le norme applicabili pertinenti

Sebbene esista un codice di condotta internazionale valido per i dati immessi nei sistemi di prenotazione computerizzati, non vi sono norme sulla tutela dei dati riguardo alle informazioni contenute nella base di dati della compagnia aerea nel paese B.

Valutazione del contenuto delle norme applicabili

Non esistono norme applicabili.

Valutazione dell'efficacia della tutela

Non applicabile.

Giudizio

I livelli di tutela nel paese B sono inadeguati, in particolare considerando la riservatezza dei dati in questione.

FASE 2: RICERCA DI UNA SOLUZIONE

Il trasferimento di dati verso il sistema di prenotazione computerizzato e la loro utilizzazione da parte della compagnia aerea allo scopo di fornire un servizio appropriato al passeggero disabile per il volo in questione è un trasferimento necessario per l'esecuzione del contratto fra il passeggero e la compa-

⁷⁷⁾ Questo caso è simile a un caso realmente avvenuto sotto la giurisdizione svedese, che ha visto coinvolte American Airlines e Lufthansa. Il caso è ancora sotto giudizio.

gnia aerea (articolo 26, paragrafo 1, lettera b). Tuttavia, la conservazione dei dati (compresi i dati riservati sulla salute dell'individuo) nella base di dati della compagnia aerea non può essere giustificata in base a questi motivi. Il trasferimento dei dati alla compagnia aerea deve quindi essere giustificato da una diversa deroga.

Come nel caso (1), la soluzione migliore è il consenso dell'interessato, che potrebbe essere ottenuto dall'agenzia di viaggi di Lisbona per conto della compagnia aerea. L'interessato va informato dei rischi derivanti dal fatto che i dati saranno conservati nel paese B, nonché del fatto che il trasferimento e la conservazione dei dati nella base di dati della compagnia aerea non sono necessari per ragioni riguardanti il volo prenotato.

CASO (3): IL TRASFERIMENTO DI DATI DI ELENCHI COMMERCIALI

Una società dei Paesi Bassi è specializzata nella creazione di «mailing lists». Utilizzando varie fonti di informazione pubblica disponibili nei Paesi Bassi e liste di clienti noleggiate da altre società olandesi, compila elenchi di persone che corrispondono a un particolare profilo socioeconomico. Questi elenchi sono poi venduti dalla società olandese a clienti nei Paesi Bassi e nell'Ue, nonché in numerosi altri paesi terzi. Le società acquirenti utilizzano gli elenchi (che comprendono indirizzi postali, numeri di telefono e spesso indirizzi di posta elettronica) per contattare le persone e proporre loro l'acquisto di una vastissima gamma di prodotti e servizi. Numerose persone che figurano su questi elenchi hanno sporto reclamo presso le autorità olandesi di tutela dei dati a causa delle proposte commerciali che hanno ricevuto.

Le norme applicabili pertinenti

Alcune delle società che hanno acquistato le «mailing lists» offerte dalla società olandese hanno sede in paesi con leggi generali sulla tutela dei dati che prevedono il diritto di rifiutare queste proposte commerciali. Altre sono situate in paesi privi di tali leggi, ma sono membri di associazioni autoregolamentate che hanno introdotto codici di protezione dei dati. Altre ancora non sono soggette ad alcuna norma sulla tutela dei dati.

Valutazione del contenuto delle norme applicabili

Questo caso specifico richiede la valutazione di una serie di leggi e di codici diversi. Se la società con sede nei Paesi Bassi continua questo tipo di vendita e di noleggio di liste a società in vari paesi del mondo, si verificheranno inevitabilmente situazioni in cui il livello di tutela non è adeguato.

FASE 2: RICERCA DI UNA SOLUZIONE

In questo caso, poiché i dati sono raccolti da fonti pubbliche e senza un contatto diretto con gli interessati, sarebbe molto problematico per la società situata nei Paesi Bassi chiedere il consenso di ogni persona alla sua inclusione nelle «mailing lists». È quindi improbabile che possa essere applicata una delle deroghe previste dall'articolo 26, paragrafo 1.

La società olandese ha due possibilità, che può utilizzare alternativamente oppure insieme. La prima è quella di limitare il suo commercio di mailing list a società soggette a giurisdizioni che garantiscono una tutela adeguata mediante

leggi o strumenti efficaci di autodisciplina. In questa sua decisione la società potrebbe essere guidata da una qualsiasi «lista bianca». La seconda possibilità sarebbe quella di chiedere un impegno contrattuale a tutte le società acquirenti (o almeno a quelle soggette a giurisdizioni «non adeguate») circa la tutela dei dati trasferiti. Questi accordi contrattuali dovrebbero seguire le indicazioni contenute nel capitolo 4 del presente documento. In virtù di tali accordi, in particolare, la società olandese dovrebbe rimanere responsabile, secondo la legislazione nazionale, di ogni violazione dei principi di tutela dei dati risultante da azioni della società cliente a cui sono state trasferite le «mailing lists».

Una tale soluzione contrattuale, se applicata in modo appropriato, contribuirebbe a superare gli ostacoli al commercio creati dalla mancanza in vari paesi terzi di una tutela adeguata dei dati.

Fatto a Bruxelles, il 24 luglio 1998

Per il gruppo di lavoro
Il presidente P.J. HUSTINX

5.7.6 Documento di lavoro sulla procedura relativa alla valutazione dei codici di condotta comunitari

COMMISSIONE EUROPEA

DIREZIONE GENERALE XV

Mercato interno e servizi finanziari

Libera circolazione delle informazioni, diritto delle società ed informazioni finanziarie

Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

DG XV D/5004/98

WP 13

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Attività futura riguardante i codici di condotta: Documento di lavoro sulla procedura relativa alla valutazione dei codici di condotta comunitari

Adottato il 10 settembre 1998

INTRODUZIONE

Il gruppo intende definire la procedura per la presentazione dei codici di condotta da parte degli interessati e per la loro valutazione ai sensi degli articoli 27 e 29 della direttiva 95/46/CE.

Nel presente documento vengono riepilogate le principali fasi della procedura e vengono definite norme specifiche per ciascuna di esse. Tali norme potranno essere riviste alla luce dell'esperienza acquisita nella loro futura applicazione.

PRINCIPALI FASI DELLA PROCEDURA

La procedura per la valutazione dell'ammissibilità e del merito dei codici di condotta si articola nelle seguenti fasi:

- I) Presentazione e ammissione;
- II) Elaborazione del parere del gruppo;
- III) Adozione del parere del gruppo e comunicazione agli interessati.

Art. 1 - Norme generali

Ai fini delle presenti norme si intende per:

1.1 «direttive»: la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, e la direttiva 97/66/CE del Parlamento Europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni;

1.2 «gruppo di tutela»: il gruppo per la tutela della persone con riguardo al trattamento dei dati personali, di cui all'articolo 29 della direttiva 95/46/CE;

1.3 «Codice di condotta»: qualsiasi codice di condotta ai sensi dell'articolo 27, § 3, della direttiva 95/46/CE nonché qualsiasi modifica e proroga di codici comunitari previgenti.

Art. 2 - Norme riguardanti la presentazione e l'ammissione dei codici per l'esame svolto dal gruppo tutelare

2.1 I progetti di codice di condotta possono essere sottoposti all'esame del gruppo tutelare da qualsiasi organizzazione rappresentativa di un determinato settore, che abbia sede od operi in un numero significativo di Stati membri.

2.2 I progetti devono essere preparati in modo accurato, preferibilmente in consultazione con le persone interessate o con i loro rappresentanti, e devono indicare chiaramente l'organizzazione o il settore cui sono destinati.

2.3 I progetti di codice devono essere inviati al presidente del gruppo di tutela - tramite il segretariato (Commissione europea, DG XV-D1) - in una lingua comunitaria e con la traduzione in lingua francese o inglese; essi devono inoltre essere corredati da una relazione illustrativa.

2.4 I progetti prematuri o comunque non conformi ai criteri sopra indicati (ai punti 1 e 2) non sono ammessi all'esame del gruppo tutelare.

2.5 Il segretariato rilascia un avviso di ricevimento all'organizzazione che ha presentato il progetto.

2.6 Previa consultazione del presidente, il segretariato redige una relazione sulla rispondenza del progetto ai criteri di ammissibilità indicati nei punti 2.1- 2.3.

2.7 Il presidente determina se il progetto risponde ai criteri di ammissibilità. Qualora constati che il progetto non risponde a tali criteri, egli informa i membri del gruppo di tutela assegnando loro un termine per la comunicazione di eventuali osservazioni. Salvo che due o più membri chiedano che la questione sia dibattuta nella successiva riunione del gruppo di tutela, la decisione del presidente viene notificata, insieme alla motivazione della valutazione negativa, all'organizzazione che ha presentato il progetto.

Art. 3 - Norme sull'elaborazione del parere del gruppo di tutela

3.1 I progetti di codice rispondenti ai criteri di ammissibilità sono trasmessi a tutti i membri del gruppo di tutela.

3.2 Sentito il presidente, il segretariato redige proposte per l'elaborazione del parere che saranno successivamente discusse dal gruppo di tutela. Tali proposte:

- possono prevedere l'istituzione di gruppi di lavoro o unità operative *ad hoc*, composti da uno o più membri del gruppo di tutela e coadiuvati dal segretariato,

- possono prevedere una procedura semplificata per l'esame di un determinato codice, segnatamente nell'ipotesi di modifica o proroga di un codice previgente, e

- consigliano il gruppo di tutela sul se e sul come raccogliere le osservazioni delle persone interessate, dei loro rappresentanti o di altri soggetti.

3.3 Nel dibattito preliminare relativo al codice sottopostogli, il gruppo di tutela definisce, in base alle proposte di cui all'articolo 3, punto 3.2, la procedura da seguire per l'adozione e l'elaborazione del parere.

3.4 Nell'ambito dell'elaborazione del parere possono tenersi consultazioni con l'organizzazione che ha presentato il progetto nonché con gli altri interessati, onde ottenere informazioni o chiarimenti ulteriori e discutere sui necessari miglioramenti da apportare al codice in vista della presentazione di un progetto modificato.

3.5 Il gruppo di tutela può stabilire ulteriori orientamenti o istruzioni per l'elaborazione del parere relativo al codice sottopostogli.

*Art. 4 - Norme riguardanti l'adozione del parere del gruppo di tutela
e la sua comunicazione agli interessati*

4.1 Il gruppo di tutela determina se il codice di condotta sottopostogli:

- è conforme alle direttive sulla tutela dei dati e, se del caso, alle disposizioni nazionali emanate per la loro attuazione;
- possiede un livello qualitativo ed una coerenza interna sufficienti e fornisce un apporto sufficiente alla disciplina stabilita dalle direttive e dagli altri provvedimenti legislativi sulla tutela dei dati, verificando in particolare se esso sia sufficientemente incentrato sulle questioni e sui problemi specifici dell'organizzazione e del settore cui è destinato e se offra soluzioni sufficientemente chiare per tali questioni o problemi.

4.2 Il gruppo di tutela comunica il parere sia all'organizzazione che ha presentato il progetto sia agli altri interessati. I pareri sfavorevoli devono contenere la motivazione della valutazione negativa.

4.3 La Commissione può dare adeguata pubblicità al parere emesso dal gruppo di tutela.

Fatto a Bruxelles, il 10 settembre 1998

Per il gruppo di tutela
Il Presidente P.J. HUSTINX

5.7.7 Parere 1/99 - Il livello di protezione dei dati negli Stati Uniti e il dibattito in corso

5092/98/EN/final
WP15

Gruppo di lavoro sulla protezione delle persone
rispetto al trattamento di dati personali

Parere 1/99: Il livello di protezione dei dati negli Stati Uniti e il dibattito in corso fra la Commissione europea e il Governo degli Stati Uniti

Adottato dal Gruppo di lavoro il 26 gennaio 1999

Il Gruppo di lavoro è a conoscenza del dibattito in corso fra la Commissione europea e il Governo degli Stati Uniti che mira a garantire sia livelli elevati di tutela per i dati personali sia la libera circolazione di dati personali fra le due sponde dell'Atlantico. Il Gruppo di lavoro attribuisce grande importanza a tale dibattito e spera che sia possibile giungere quanto prima a risultati positivi. Alla luce del dibattito in oggetto, è stata trasmessa una lettera con il relativo allegato a firma del sottosegretario Aaron, del 4 novembre 1998, contenente una serie di proposte destinate ad essere discusse negli USA fra rappresentanti di imprese statunitensi e il Federal Department of Commerce. In questo contesto, il Gruppo di lavoro invita i soggetti partecipanti a tale discussione ed i governi degli Stati membri dell'UE riuniti nel comitato istituito ai sensi dell'articolo 31 della Direttiva 95/46/CE⁷⁸⁾ a tenere presenti i punti di seguito indicati.

Le norme in materia di protezione dei dati non mirano esclusivamente a tutelare gli utilizzatori di nuove tecnologie (in particolare informatica e Internet) al fine di garantire fiducia e sicurezza e quindi contribuire allo sviluppo di tali tecnologie ed allo scambio di dati a livello internazionale. Queste norme esprimono anche l'adesione a una serie di principi e diritti fondamentali basati su una cultura comune di rispetto per la *privacy* ed altri valori propri degli esseri umani, che è condivisa allo stesso modo dagli Stati membri dell'Unione europea e dagli Stati Uniti.

1. Negli Stati Uniti, *privacy* e protezione dei dati sono rinvenibili in un complesso intreccio di regolamentazione settoriale, a livello sia federale sia statale, unita all'autoregolamentazione da parte delle imprese. Negli ultimi mesi sono stati compiuti sforzi notevoli per migliorare credibilità ed applicabilità dell'autoregolamentazione da parte delle imprese, particolarmente nell'ambito di Internet e del commercio elettronico. Tuttavia, il Gruppo di lavoro è del parere che al momento non si possa fare affidamento sull'attuale collage di legislazione settoriale ad alta specificità e autoregolamentazione su base volontaria quale garanzia di una protezione adeguata in tutti i casi di trasferimento di dati personali dall'Unione europea.

⁷⁸⁾ Direttiva 95/46/EC del Parlamento europeo e del Consiglio del 24 ottobre 1995 sulla protezione delle persone rispetto al trattamento di dati personali e sulla libera circolazione di tali dati. GU L 281, 23 novembre 1995.

2. Data la complessità dell'attuale sistema statunitense di tutela della *privacy* e dei dati, la definizione negli USA di uno standard concordato «di riferimento» per tale tutela, sotto forma di una serie di principi che rappresentino un «porto sicuro» e siano offerti a tutti i soggetti economici ed agli operatori statunitensi, costituisce un utile approccio che, in determinati casi, potrebbe necessitare di integrazioni attraverso soluzioni contrattuali. Tuttavia, occorrono miglioramenti ulteriori per garantire la libera circolazione di dati verso gli Stati Uniti sulla base di questi principi in materia di *privacy*. Inoltre, potrebbe risultare necessario prevedere una metodologia che chiarisca quali sono le imprese per le quali valgono i principi del «porto sicuro».

3. Si deve osservare che la decisione di aderire a questo insieme di principi spetta esclusivamente alla singola impresa, per cui resta il problema costituito dalle imprese che non desiderano applicare i principi in oggetto, in assenza di una legislazione generale in materia.

4. In via generale, occorre chiarire la natura di questi principi. L'adesione ai principi può essere volontaria in prima istanza, ma una volta che un'impresa abbia deciso di aderire e quindi di usufruire dei vantaggi del «porto sicuro», il rispetto dei principi deve essere obbligatorio.

5. La credibilità dell'intero sistema risulta gravemente compromessa dall'assenza del requisito di un monitoraggio indipendente del rispetto dei principi, e dalla circostanza per cui si fa esclusivo affidamento sull'autocertificazione delle imprese. Il controllo indipendente sarebbe necessariamente serio, ma al contempo potrebbe essere fattibile, anche per le piccole imprese. I modelli in via di definizione negli USA ad opera di Better Business Bureau OnLine e di TrustE vanno nella direzione giusta.

6. Deve essere possibile che i reclami presentati da soggetti i cui dati sono stati trasferiti dall'Unione europea vengano gestiti in modo fattivo ed efficiente, e che la decisione in merito sia presa, in ultima istanza, da un organismo indipendente. A tale riguardo, un punto fondamentale è l'individuazione di uno o più enti pubblici indipendenti ovvero organismi terzi, negli USA, che siano disposti a ed in grado di fungere da punti di contatto per le autorità preposte alla protezione dei dati nell'Ue, collaborando negli accertamenti relativi a tali reclami. Si deve fare in modo di garantire l'esistenza di disposizioni pratiche per tutti i settori pertinenti negli USA. Gli organismi di regolamentazione già esistenti, quali la Federal Trade Commission e l'Office of the Comptroller of the Currency, possono svolgere questa funzione nei settori di competenza.

7. Alla luce del contenuto sostanziale, qualsiasi insieme accettabile di principi costituenti un «porto sicuro» deve comprendere, quale requisito minimo, tutti i principi fissati nelle Linee-guida in materia di *privacy* elaborate dall'OCSE nel 1980, adottate, fra gli altri, dagli USA e recentemente ribadite nel corso della Conferenza OCSE di Ottawa sul commercio elettronico. Questi principi trovano applicazione anche nella Direttiva 95/46/CE e nella normativa nazionale degli Stati membri dell'Unione europea. A tale riguardo, il documento di consultazione sopra ricordato, relativo ai principi, pubblicato dal Department of Commerce degli USA il 4 novembre 1998, suscita alcune perplessità, e in particolare:

a) Il diritto di accesso dei singoli è limitato a quanto è «ragionevole». Le Linee-guida dell'OCSE in materia di *privacy* non prevedono limitazioni a questo diritto in quanto tale, affermando più semplicemente che esso deve essere esercitato «in modo ragionevole».

b) Manca ogni riferimento al principio per cui le finalità del trattamento devono essere conformi, contenuto nelle Linee-guida dell'OCSE in materia di *privacy*, che è sostituito solo in parte da un principio di «scelta» per cui, di fatto, dati raccolti per un determinato scopo possono essere utilizzati per un altro scopo, purché i singoli abbiano la possibilità di «chiamarsi fuori» (*opt-out*).

c) I dati protetti dal diritto d'autore ed i dati sottoposti a trattamento non automatizzato sono del tutto esclusi dall'ambito di applicazione dei principi USA, mentre il principio di «scelta» non offre alcuna tutela per i dati raccolti presso terzi, e il principio di «accesso» esclude i dati ricavabili da atti pubblici.

d) In base al terzo paragrafo dell'introduzione, «l'adesione ai principi è subordinata» a una serie di eccezioni e limitazioni quali la «gestione dei rischi», e la «sicurezza delle informazioni». Il Gruppo di lavoro è del parere che si tratti di concetti eccessivamente vaghi e indefiniti, e ne raccomanda un chiarimento o l'eliminazione.

Fatto a Bruxelles il 26 gennaio 1999

Per il Gruppo di lavoro
Il Presidente: Prof. Stefano RODOTÀ

5.8 COMMISSIONE EUROPEA

5.8.1 Progetto di direttiva per le firme elettroniche ⁷⁹⁾

UNIONE EUROPEA

Bruxelles, 19 novembre 1998 (24.11)

IL CONSIGLIO

(Or. en)

13189/98

LIMITE

ECO 418

CODEC 635

Risultati dei lavori

del : COREPER

in data : 18 novembre 1998

al : CONSIGLIO «TELECOMUNICAZIONI»

n. doc. prec. : 12935/98 ECO 406 CODEC 603

n. prop. Comm. : 9708/98 ECO 233 CODEC 355

Presentato al Consiglio «Telecomunicazioni» del 27 novembre 1998 ⁸⁰⁾.

OGGETTO: Progetto di direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comune per le firme elettroniche

Progetto di direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comune per le firme elettroniche

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA

Visto il trattato che istituisce la Comunità europea, in particolare l'articolo 57, paragrafo 2, l'articolo 66 e l'articolo 100 A,

Vista la proposta della Commissione,

Visto il parere del Comitato economico e sociale,

Visto il parere del Comitato delle regioni,

Deliberando in conformità della procedura di cui all'articolo 189 B del trattato,

1) considerando che il 16 aprile 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni una comunicazione intitolata «Un'iniziativa europea in materia di commercio elettronico»;

⁷⁹⁾ Ultimo testo disponibile in lingua italiana.

⁸⁰⁾ Ultimo testo disponibile in lingua italiana.

2) considerando che l'8 ottobre 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni la comunicazione intitolata «Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche - Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura»;

3) considerando che il 1° dicembre 1997 il Consiglio ha invitato la Commissione a presentare quanto prima una proposta di direttiva del Parlamento europeo e del Consiglio relativa alle firme digitali;

4) considerando che le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati; che la divergenza delle regole in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico e, di conseguenza, impedire lo sviluppo del mercato interno; che la divergenza degli interventi negli Stati membri sottolinea l'esigenza di un'armonizzazione a livello comunitario;

5) considerando che occorre promuovere l'interoperabilità dei prodotti di firma elettronica; che ai sensi dell'articolo 7 A del trattato, il mercato interno comporta uno spazio senza frontiere interne, nel quale deve essere assicurata la libera circolazione delle merci; che per garantire la libera circolazione nell'ambito del mercato interno e per infondere fiducia nelle firme elettroniche è necessaria la conformità ai requisiti essenziali specifici relativi ai prodotti di firma elettronica utilizzati dai fornitori di servizi di certificazione;

6) considerando che la rapida evoluzione tecnologica e il carattere globale di Internet rendono necessario un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico; che tuttavia, le firme digitali basate sulla crittografia a chiave pubblica costituiscono attualmente la forma più riconosciuta di firma elettronica;

7) considerando che il mercato interno consente ai prestatori di servizi di certificazione di sviluppare le proprie attività transfrontaliere ai fini di accrescere la competitività, e pertanto di offrire ai consumatori e alle imprese nuove opportunità di scambiare informazioni e di effettuare negozi per via elettronica in modo sicuro, indipendentemente dalle frontiere; che al fine di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte, i prestatori di servizi di certificazione debbono essere generalmente liberi di offrire i rispettivi servizi senza preventiva autorizzazione; che non vi è immediata necessità di garantire la libera circolazione dei servizi di certificazione armonizzando le disposizioni nazionali che impongono restrizioni giustificate e proporzionate alla prestazione di tali servizi;

8) considerando che i sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito possono offrire ai prestatori di servizi di certificazione il contesto appropriato per l'ulteriore sviluppo dei loro servizi verso i livelli di fiducia, sicurezza e qualità richiesti dall'evoluzione del mercato; che tali sistemi debbono incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; che questi ultimi debbono essere liberi di aderire a tali sistemi di accreditamento e di trarne vantaggio; che gli Stati membri non debbono vietare ai prestatori di servizi di certificazione di operare al di fuori di tali sistemi di accreditamento; che si deve garantire che i sistemi di accredita-

mento non riducano la concorrenza nel settore dei servizi di certificazione; che è importante raggiungere l'equilibrio tra esigenze dei consumatori ed esigenze delle imprese;

9) considerando che la presente direttiva contribuisce pertanto all'uso e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità; che le firme elettroniche usate esclusivamente all'interno di sistemi chiusi non esigono una disciplina comune; che, nella misura consentita dal diritto nazionale, va rispettata la libertà delle parti di accordarsi sulle condizioni di accettazione dei dati firmati in modo elettronico; che la presente direttiva non è intesa ad armonizzare le normative nazionali sui contratti, in particolare in materia di formazione ed esecuzione dei contratti, od altre formalità non contrattuali che richiedano l'apposizione di firme; che per tale motivo, le disposizioni sugli effetti giuridici delle firme elettroniche non devono riguardare i requisiti legali di forma previsti dal diritto nazionale sulla conclusione dei contratti o le regole di determinazione del luogo della conclusione del contratto;

10) considerando che, al fine di contribuire all'accettazione generale delle firme elettroniche, la validità giuridica di una firma elettronica non deve essere disconosciuta unicamente per il fatto che si presenta sotto forma di dati elettronici, oppure che essa non è basata su un certificato qualificato o su un certificato rilasciato da un prestatore di servizi di certificazione accreditato, oppure per il fatto che il prestatore di servizi che ha rilasciato il relativo certificato appartiene ad un altro Stato membro; che le firme elettroniche connesse ad un prestatore di servizi di certificazione affidabile che si conformi ai requisiti essenziali debbono avere la stessa efficacia giuridica delle firme autografe; che è necessario garantire che le firme elettroniche possano essere utilizzate come prove nei procedimenti giudiziari in tutti gli Stati membri; che il riconoscimento giuridico delle firme elettroniche deve basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione rilasciata al prestatore di servizi interessato; che regole armonizzate relative all'efficacia giuridica delle firme elettroniche devono garantire una disciplina giuridica coerente in tutta la Comunità;

11) considerando che la responsabilità dei prestatori di servizi di certificazione che offrono tali servizi al pubblico è disciplinata dal diritto nazionale; che l'eterogeneità della portata e del contenuto di tali regole può compromettere la certezza del diritto, soprattutto per quanto riguarda i terzi che si affidano ai servizi dei citati prestatori; che tale incertezza può danneggiare lo sviluppo del commercio transfrontaliero e ostacolare il corretto funzionamento del mercato interno; che l'armonizzazione delle regole in materia di responsabilità garantisce la sicurezza e la prevedibilità sul piano giuridico sia per i prestatori di servizi di certificazione, sia per i consumatori; che tali regole contribuiranno all'accettazione generale e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità, e di conseguenza influiranno positivamente sul funzionamento del mercato interno;

12) considerando che lo sviluppo del commercio elettronico internazionale rende necessari dispositivi transfrontalieri che coinvolgono i paesi terzi; che tali dispositivi dovrebbero essere elaborati a livello commerciale; che al fine di garantire l'interoperabilità a livello globale, potrebbe essere utile stipulare accordi con i paesi terzi relativi a regole multilaterali per il reciproco riconoscimento dei servizi di certificazione;

13) considerando che al fine di stimolare le comunicazioni elettroniche e il commercio elettronico garantendo la fiducia da parte degli utenti, gli Stati membri debbono obbligare i prestatori di servizi di certificazione a rispettare la-

legislazione in materia di protezione dei dati e la vita privata degli individui, e debbono richiedere a questi ultimi di fornire, qualora il firmatario lo richieda, anche servizi di certificazione relativi a pseudonimi; che il diritto nazionale deve stabilire in quali casi e a quali condizioni i dati che rivelano l'identità della persona cui i dati medesimi si riferiscono debbano essere trasferiti ai fini di inchieste penali; che i prestatori di servizi di certificazione debbono informare preventivamente gli utenti, per iscritto e in termini facilmente comprensibili e utilizzando mezzi di comunicazione durevoli, in merito alle condizioni praticate, in particolare alle precise modalità d'uso dei certificati rilasciati ed ai limiti della loro responsabilità;

14) considerando che ai fini dell'applicazione della presente direttiva la Commissione deve essere assistita da un comitato a carattere consultivo;

15) considerando che, conformemente ai principi di sussidiarietà e proporzionalità di cui all'articolo 3 B del trattato, l'obiettivo di un quadro giuridico armonizzato per la prestazione di firme elettroniche e dei servizi ad esse relativi non può essere sufficientemente realizzato dagli Stati membri e può pertanto essere meglio realizzato a livello comunitario; che la presente direttiva si limita ai requisiti minimi essenziali per la realizzazione di tale obiettivo e non esula da ciò che è necessario a questo scopo,

HANNO ADOTTATO LA PRESENTE DIRETTIVA

Art. 1

*Campo di applicazione*⁸¹⁾

La presente direttiva è intesa ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico. Essa istituisce un quadro giuridico per le firme elettroniche e taluni servizi di certificazione al fine di garantire il corretto funzionamento del mercato interno.

Essa non disciplina aspetti relativi alla conclusione e alla validità dei contratti o altri obblighi giuridici quando esistono requisiti di forma prescritti dal diritto nazionale o comunitario, né pregiudica le norme e i limiti che disciplinano l'uso dei documenti contenuti nel diritto nazionale o comunitario.

Art. 2

Definizioni

Ai fini della presente direttiva, valgono le seguenti definizioni:

1. «firma elettronica», dati in forma elettronica allegati, oppure connessi tramite associazione logica, ad altri dati elettronici, utilizzata come metodo di autenticazione⁸²⁾.

⁸¹⁾ Considerando supplementare che dovrà essere confermato dopo il Consiglio: «considerando che la presente direttiva fa salve le disposizioni nazionali inerenti all'ordine e alla sicurezza pubblici o relative alla fornitura di servizi intesi a garantire la riservatezza».

⁸²⁾ Riserva di F.

1-*bis* «firma elettronica avanzata», una firma elettronica che soddisfi i seguenti requisiti:

- a) essere connessa esclusivamente al firmatario;
- b) essere idonea ad identificare il firmatario;
- c) essere creata con mezzi sui quali il firmatario può conservare il proprio esclusivo controllo;
- d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva alterazione⁸³⁾ di detti dati.

2. «firmatario», colui che detiene un dispositivo per la creazione di una firma e agisce o per se stesso o per conto dell'entità da esso rappresentata.

3. «dispositivo per la creazione di una firma», dati peculiari, come codici o chiavi crittografiche private, oppure un dispositivo materiale di configurazione esclusiva utilizzato dal firmatario per creare una firma elettronica.

4. «dispositivo di verifica della firma», dati, come codici o chiavi crittografiche pubbliche, oppure un dispositivo materiale di configurazione utilizzato per verificare la firma elettronica;

4-*bis* «certificato», un attestato digitale che collega un dispositivo di verifica della firma ad una data persona e conferma l'identità di tale persona;

5. «certificato qualificato», un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;

6. «prestatore di servizi di certificazione»⁸⁴⁾, una persona o un'entità che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche⁸⁵⁾.

7. «prodotto di firma elettronica», macchinari o programmi per elaboratori elettronici, oppure i componenti pertinenti dei medesimi destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica.

⁸³⁾ Riserva di *UK*.

⁸⁴⁾ Considerando supplementare che dovrà essere esaminato dopo il Consiglio: «Considerando che i servizi di certificazione possono essere offerti o da un'entità pubblica ovvero da una persona giuridica o fisica, stabilita a norma della legislazione nazionale.»

⁸⁵⁾ È stato concordato il seguente considerando supplementare (all'inizio del considerando n.7):

«considerando che le firme elettroniche verranno usate in una grande varietà di circostanze ed applicazioni, che comporteranno un'ampia gamma di nuovi servizi e prodotti facenti uso di firme elettroniche o ad esse collegati;

che la definizione di tali prodotti e servizi non dovrebbe essere limitata al rilascio e alla gestione di certificati, ma comprendere anche ogni altro servizio e prodotto facente uso di firme elettroniche o ad esse ausiliario, quali servizi di immatricolazione, servizi di apposizione del giorno e dell'ora, servizi di repertorizzazione, servizi informatici o consulenza relativi alle firme elettroniche;

che la libera circolazione di tutti i suddetti prodotti e servizi deve essere assicurata conformemente alle disposizioni del trattato;».

Art. 3

Accesso al mercato

1. Gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione ⁸⁶⁾.

2. Salvo il disposto del paragrafo 1, gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi ⁸⁷⁾ intesi a fornire servizi di certificazione di livello più elevato. Tutte le condizioni relative a tali sistemi devono essere obiettive, trasparenti, proporzionate e non discriminatorie. Gli Stati membri non possono limitare il numero di prestatori di servizi di certificazione accreditati per motivi che rientrano nel campo d'applicazione della presente direttiva.

2-bis Gli Stati membri provvedono affinché venga istituito un sistema appropriato che consenta il controllo dei prestatori di servizi di certificazione stabiliti nel loro territorio che rilasciano certificati qualificati al pubblico ⁸⁸⁾.

3. Secondo la procedura di cui all'articolo 9, la Commissione può determinare e pubblicare sulla Gazzetta ufficiale delle Comunità europee i numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica. Un prodotto di firma elettronica conforme a tali norme viene considerato dagli Stati membri conforme ai requisiti di cui all'allegato II, punto e) [e allegato III].

4. Gli Stati membri possono assoggettare ad eventuali requisiti supplementari l'uso delle firme elettroniche ⁸⁹⁾, nel settore pubblico. Tali requisiti debbono essere obiettivi, trasparenti, proporzionati e non discriminatori, e riguardare unicamente le caratteristiche specifiche dell'uso di cui trattasi.

⁸⁶⁾ Considerando supplementare che dovrà essere esaminato dopo il Consiglio: «considerando che per autorizzazione preventiva non s'intende solo qualsiasi permesso che imponga al prestatore di servizi di certificazione interessato di ottenere dalle autorità nazionali una decisione prima di essere autorizzato a prestare i propri servizi di certificazione, ma anche ogni altro requisito il cui effetto sia di rendere tale disposizione dipendente da una decisione, una misura o un atto specifico da parte di un'autorità nazionale;»

⁸⁷⁾ È stato concordato il seguente considerando: «considerando che per accreditamento facoltativo si intende qualsiasi permesso, che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione, dall'autorità incaricata dell'elaborazione e della sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'autorità».

⁸⁸⁾ È stato concordato il seguente considerando: «considerando che gli Stati membri possono decidere come garantire il controllo del rispetto delle disposizioni contenute nella presente direttiva; che la direttiva non esclude l'istituzione di sistemi di controllo basati nel settore privato;». Tuttavia dovrebbe essere presa in considerazione dopo il Consiglio la seguente aggiunta: «Considerando che la presente direttiva non obbliga i prestatori di servizi di certificazione a chiedere il controllo in base a un qualsiasi accordo d'accredimento o licenza.».

⁸⁹⁾ Considerando supplementare che dovrà essere confermato dopo il Consiglio: «considerando che le firme elettroniche saranno utilizzate nel settore pubblico nell'ambito delle amministrazioni nazionali e comunitarie e nelle comunicazioni tra tali amministrazioni nonché con i cittadini e gli operatori economici, ad esempio nei settori degli appalti pubblici, della fiscalità, della sicurezza sociale, della sanità e dell'amministrazione della giustizia;».

Art. 4

Principi del mercato interno

1. Ciascuno Stato membro applica le norme di attuazione della presente direttiva ai prestatori di servizi di certificazione stabiliti sul suo territorio e ai servizi da essi forniti. Gli Stati membri non possono limitare la prestazione di servizi di certificazione originati in un altro Stato membro nella materia disciplinata dalla presente direttiva.

2. Gli Stati membri provvedono a che i prodotti di firma elettronica conformi alla presente direttiva circolino liberamente nel mercato interno ⁹⁰⁾.

Art. 5

Effetti giuridici ⁹¹⁾

1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato [e che sono create da dispositivi che soddisfano ai requisiti di cui all'allegato III] ⁹²⁾:

a) soddisfino i requisiti giuridici di una firma in relazione ai dati in forma elettronica così come una firma autografa soddisfa tali requisiti in relazione a dati cartacei;

b) siano ammesse come prova nei procedimenti giudiziari.

2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata inefficace e inammissibile come prova nei procedimenti giudiziari unicamente a causa della sua forma elettronica, o per il fatto che non è basata su un certificato qualificato o su un certificato rilasciato da un prestatore di servizi di certificazione accreditato ⁹³⁾ [ovvero non è creata da un dispositivo per la creazione di una firma che soddisfa ai requisiti di cui all'allegato III].

⁹⁰⁾ È stato concordato di riformulare questo considerando:

«considerando che dovrebbe essere promossa l'interoperabilità dei prodotti di firma elettronica; che, a norma dell'articolo 7A del trattato, il mercato interno dovrà comprendere una zona in cui sarà assicurata la libera circolazione delle merci; che i requisiti fondamentali propri dei prodotti di firma elettronica usati dai prestatori di servizi di certificazione devono essere soddisfatti per garantire la libera circolazione nel mercato interno e creare la fiducia nelle firme elettroniche, fatto salvo il regolamento (CE) n. 3381/94 che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso e la decisione 94/942/CFSP relativa all'azione comune, adottata dal Consiglio in base all'articolo J.3 del trattato sull'Unione europea, riguardante il controllo dell'esportazione dei beni a duplice uso;».

⁹¹⁾ È stato concordato il seguente considerando:

«considerando che il diritto nazionale disciplina l'uso dei documenti elettronici e delle firme elettroniche;».

⁹²⁾ È stato concordato il seguente considerando:

«considerando che il diritto nazionale disciplina l'uso dei documenti elettronici e delle firme elettroniche;».

⁹³⁾ Considerando supplementare che dovrà essere confermato dopo il Consiglio:

«considerando che la presente direttiva non ha lo scopo di interferire con le norme nazionali in materia di libero uso delle prove in sede giudiziaria».

Art. 6

*Responsabilità*⁹⁴⁾

Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico un certificato, sia responsabile per danni provocati a chiunque faccia ragionevole affidamento sul certificato in questione, per quanto riguarda:

a) l'esattezza di tutte le informazioni contenute nel certificato qualificato a partire dalla data di rilascio,

b) [...]

c) la garanzia che, al momento del rilascio del certificato, il titolare identificato nel certificato qualificato detenesse il dispositivo di creazione della firma corrispondente al dispositivo di verifica della firma riportato o identificato nel certificato;

d) la garanzia che il dispositivo di creazione della firma e il dispositivo di verifica della firma, garanzia che i due dispositivi funzionino insieme in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi i due dispositivi.

a meno che il prestatore di servizi di certificazione non provi di non aver agito con negligenza.

1-bis. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato sia responsabile, nei confronti di chiunque faccia ragionevole affidamento sul certificato, dei danni provocatigli, tra cui la mancata registrazione della revoca del certificato, a meno che non provi di non aver agito con negligenza.

2. Gli Stati membri provvedono a che un prestatore di servizi di certificazione sia esentato dalla responsabilità derivante da eventuali errori contenuti nelle informazioni riportate nel certificato qualificato e a suo tempo fornite dalla persona cui è stato rilasciato il certificato, qualora detto prestatore possa dimostrare di aver usato tutta la necessaria diligenza per verificare tali informazioni.

3. Gli Stati membri provvedono a che un prestatore di servizi di certificazione possa indicare, nel certificato qualificato, i limiti d'uso di un determinato certificato. Il prestatore di servizi di certificazione deve essere esentato dalla responsabilità per i danni derivanti dall'uso indebito di un certificato qualificato ove siano precisati i limiti d'uso dello stesso.

4. Gli Stati membri provvedono affinché un prestatore di servizi di certificazione abbia la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato.

5. I paragrafi da 1 a 4 si applicano salvo il dispositivo della direttiva 93/13/CE del Consiglio.

⁹⁴⁾ Considerando supplementare che dovrà essere confermato dopo il Consiglio:
«considerando che la presente direttiva non pregiudica alcun diritto di cui una persona che faccia affidamento su un certificato possa godere conformemente alle disposizioni della legislazione sulla responsabilità contrattuale o extracontrattuale o a un regime di responsabilità particolare esistente al momento dell'entrata in vigore della direttiva».

Art. 7***Aspetti internazionali***

1. Gli Stati membri provvedono a che i certificati rilasciati al pubblico come certificati qualificati da un prestatore di servizi di certificazione stabilito in un paese terzo siano riconosciuti come equivalenti, sul piano giuridico, ai certificati rilasciati da un prestatore di servizi di certificazione stabilito nella Comunità europea, in presenza di una delle seguenti condizioni:

a) qualora il prestatore di servizi di certificazione soddisfi i requisiti di cui alla presente direttiva e sia stato accreditato nel contesto di un sistema di accreditamento facoltativo stabilito in uno Stato membro della Comunità europea, oppure

b) qualora il prestatore di servizi di certificazione stabilito nella Comunità, che soddisfa i requisiti della presente direttiva, garantisca il certificato; oppure

c) qualora il certificato o il prestatore di servizi di certificazione sia riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e paesi terzi o organizzazioni internazionali.

2. Al fine di agevolare servizi di certificazione transfrontalieri con paesi terzi e il riconoscimento giuridico delle firme elettroniche avanzate che hanno origine in paesi terzi, la Commissione presenterà se del caso, proposte miranti all'effettiva attuazione di norme e di accordi internazionali sui servizi di certificazione. In particolare, ove necessario, presenterà al Consiglio proposte relative a mandati per la negoziazione di accordi bilaterali e multilaterali con paesi terzi e organizzazioni internazionali. Il Consiglio decide a maggioranza qualificata.

3. Ogniquale volta la Commissione è informata di difficoltà che le imprese comunitarie incontrano riguardo all'immissione sul mercato di paesi terzi, essa può, se necessario, presentare al Consiglio proposte in merito a un appropriato mandato negoziato per ottenere diritti paragonabili per le imprese comunitarie in tali paesi terzi.

Le misure adottate a norma di questo paragrafo lasciano impregiudicati gli obblighi della Comunità e degli Stati membri derivanti da accordi internazionali in materia.

Art. 8***Protezione dei dati***

1. Gli Stati membri provvedono a che i prestatori di servizi di certificazione e gli organismi nazionali responsabili dell'accreditamento o della supervisione si conformino alla direttiva 95/46/CE del Parlamento europeo e del Consiglio.

2. Gli Stati membri provvedono a che un prestatore di servizi di certificazione che rilascia certificati al pubblico possa raccogliere dati personali unicamente in via diretta dalla persona cui i dati si riferiscono o con il suo esplicito consenso, e unicamente nella misura in cui ciò sia necessario ai fini del rilascio e del mantenimento del certificato. I dati non possono essere raccolti o elaborati per fini diversi senza l'esplicito consenso della persona cui essi si riferiscono.

3. Fatti salvi gli effetti giuridici che la legislazione nazionale attribuisce allo psesudonimo, gli Stati membri non vietano al prestatore di servizi di certificazione di riportare sul certificato uno pseudonimo in luogo del nome del firmatario⁹⁵⁾.

4. [...]

Art. 9

Comitato

La Commissione è assistita da un Comitato a carattere consultivo, denominato «Comitato per la firma elettronica» (in prosieguo: «il Comitato»), composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione.

Il rappresentante della Commissione sottopone al Comitato un progetto delle misure da adottare. Il Comitato, entro un termine che il Presidente può fissare in funzione dell'urgenza della questione in esame, formula il suo parere sul progetto. Il parere è formulato alla maggioranza prevista all'articolo 148, paragrafo 2 del trattato per l'adozione delle decisioni che il Consiglio deve prendere su proposta della Commissione. Nelle votazioni in seno al Comitato, ai voti dei rappresentanti degli Stati membri è attribuita la ponderazione fissata nell'articolo precitato. Il presidente non partecipa al voto.

La Commissione adotta misure che sono immediatamente applicabili. Tuttavia, se tali misure non sono conformi al parere espresso dal Comitato, la Commissione le comunica immediatamente al Consiglio. In tal caso:

La Commissione differisce l'applicazione delle misure da essa decise di un periodo da fissare in ogni atto adottato dal Consiglio, ma che in ogni modo non potrà superare tre mesi a decorrere dalla data della comunicazione.

Il Consiglio, deliberando a maggioranza qualificata, può prendere una decisione diversa entro il termine di cui al comma precedente.

Art. 10

Consultazione del Comitato

Il Comitato è consultato sulla delucidazione dei requisiti di cui agli allegati e in merito alle norme generalmente riconosciute per i prodotti di firma elettronica, a norma dell'articolo 3, paragrafo 3.

Art. 11

Notificazione

1. Gli Stati membri comunicano alla Commissione, che a sua volta ne informa gli altri Stati membri, le informazioni relative a quanto segue:

a) sistemi di accreditamento facoltativi nazionali ed ogni requisito supplementare a norma dell'articolo 3, paragrafo 4;

⁹⁵⁾ Riserva di I e riserva d'esame di UK.

Considerando supplementare che dovrà essere esaminato dopo il Consiglio: «considerando che la disposizione sull'uso degli pseudonimi nei certificati non vieta agli Stati membri di chiedere l'identificazione delle persone a norma della normativa comunitaria o della legislazione nazionale».

b) nomi e indirizzi degli enti nazionali responsabili dell'accreditamento e della supervisione;

c) i nomi e gli indirizzi di tutti i prestatori di servizi di certificazione nazionali accreditati.

2. Gli Stati membri notificano al più presto le informazioni di cui al paragrafo 1 nonché le eventuali variazioni.

Art. 12

Riesame

1. Entro [...], la Commissione, previo esame dell'applicazione della presente direttiva, presenta una relazione in merito al Parlamento europeo e al Consiglio.

2. Nel riesame si valuta, *tra l'altro*, se il campo d'applicazione della direttiva debba essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi sul piano giuridico. La relazione include segnatamente una valutazione, sulla base dell'esperienza acquisita, degli aspetti relativi all'armonizzazione. La relazione è accompagnata, se del caso, da proposte legislative complementari.

Art. 13

Attuazione

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il [...] ⁹⁶⁾. Essi ne informano immediatamente la Commissione.

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate da un siffatto riferimento all'atto della pubblicazione ufficiale. Gli Stati membri adottano la procedura per tale riferimento.

2. Gli Stati membri comunicano alla Commissione le disposizioni di diritto nazionale che adottano nella materia disciplinata dalla presente direttiva.

Art. 14

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla data della sua pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

Art. 15

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, il

PER IL PARLAMENTO EUROPEO

Il Presidente

PER IL CONSIGLIO

Il Presidente

⁹⁶⁾ Entro [x] mesi dall'entrata in vigore della presente direttiva.

*ALLEGATO I***REQUISITI RELATIVI AI CERTIFICATI QUALIFICATI**

I certificati qualificati devono includere:

- x) l'indicazione se il certificato rilasciato è un certificato qualificato;
 - a) l'identificazione del paese di stabilimento del prestatore di servizio di certificazione che ha rilasciato il certificato in questione;
 - b) il nome del titolare del certificato o uno pseudonimo identificato come tale;
 - c) l'indicazione di un attributo specifico del titolare, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;
 - d) un dispositivo di verifica della firma che corrisponda ad un dispositivo di creazione della firma sotto il controllo del titolare;
 - e) l'inizio e il termine del periodo di validità del certificato;
 - f) il codice d'identificazione esclusivo del certificato;
 - g) la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;
 - h) i limiti d'uso del certificato, ove applicabili;
 - i) i limiti dell'importo delle transazioni per cui il certificato può essere usato, ove applicabili.
-

*ALLEGATO II***REQUISITI RELATIVI AI PRESTATORI DI SERVIZI DI CERTIFICAZIONE
CHE RILASCIANO CERTIFICATI QUALIFICATI**

I prestatori di servizi di certificazione devono:

- a) dimostrare l'affidabilità necessaria per fornire servizi di certificazione;
- b) assicurare il funzionamento di un servizio di repertorizzazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;
- c) verificare con mezzi appropriati l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato;
- d) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi offerti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la familiarità con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute;
- e) utilizzare sistemi affidabili e usare prodotti di firma elettronica che garantiscano la protezione contro alterazioni dei prodotti, di modo che non sia possibile utilizzarli per funzioni diverse da quelle per cui sono stati progettati; essi debbono inoltre utilizzare prodotti di firma elettronica che garantiscano la sicurezza tecnica e crittografica dei procedimenti di certificazione di cui sono oggetto i prodotti in questione;
- f) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi chiavi private di firma crittografica, garantire la riservatezza nel corso della generazione di tali chiavi;

g) disporre di risorse finanziarie sufficienti ad operare in conformità dei requisiti previsti dalla presente direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione;

h) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare ai fini di prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere effettuate per via elettronica;

i) astenersi dal memorizzare o dal copiare le chiavi private di firma crittografica della persona cui il prestatore di servizi di certificazione ha offerto i servizi di gestione della chiave⁹⁷⁾;

j) «prima di avviare una relazione contrattuale con una persona che desideri ottenere un certificato a sostegno della sua firma elettronica, informare questa persona utilizzando un mezzo di comunicazione durevole, in merito agli esatti termini e condizioni d'uso del certificato, inclusa ogni limitazione dell'uso, l'esistenza di un accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, sono fornite per iscritto, possono essere trasmesse elettronicamente e devono utilizzare un linguaggio comprensibile. Su richieste, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato»;

k) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:

- soltanto le persone autorizzate possano effettuare inserimenti e modifiche;

- le informazioni possano, essere controllate per stabilirne l'autenticità;

- i certificati siano accessibili alla consultazione del pubblico soltanto previo assenso del titolare del certificato;

- l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

ALLEGATO III

REQUISITI RELATIVI

AI DISPOSITIVI PER LA CREAZIONE DELLA FIRMA ELETTRONICA

I dispositivi per la creazione della firma assicurano, entro limiti ragionevoli di certezza, mediante strumenti tecnici e procedurali appropriati, che

a) i dati per la creazione della firma utilizzati nella generazione della stessa compaiano, pressoché invariabilmente, solo una volta e che sia ragionevolmente garantita la confidenzialità della firma;

⁹⁷⁾ Nuovo considerando che dovrà essere confermato dopo il Consiglio:

«considerando che la memorizzazione e la copia delle chiavi private di firma crittografica della persona cui il prestatore di servizi di certificazione ha offerto i servizi di gestione della chiave potrebbero compromettere seriamente la validità giuridica delle firme crittografiche; che la presente direttiva vieta ai prestatori di servizi di certificazione che offrono al pubblico certificati qualificati di memorizzare o copiare chiavi private di firma crittografica; che la facoltà di vietare ai prestatori di servizi di certificazione la memorizzazione o la copia di tali chiavi è lasciata agli Stati membri;».

b) i dati per la creazione della firma utilizzati nella generazione della stessa non siano derivati e che la firma non sia contraffatta con mezzi normalmente utilizzati;

c) i dati per la creazione della firma utilizzati nella generazione della stessa siano sufficientemente protetti dal titolare legittimo contro l'uso da parte di terzi;

d) il firmatario sia consapevole del processo relativo alla firma che precede l'attivazione della funzione di quest'ultima e possa determinare in modo attendibile i dati cui fa riferimento la firma in questione;

e) i dati da usare per la firma corrispondano ai dati comunicati al firmatario;

f) il firmatario possa eventualmente, se necessario, determinare in modo affidabile i contenuti dei dati da usare per la firma;

g) possa essere individuata qualsiasi modifica pertinente.⁹⁸⁾

⁹⁸⁾ Cfr. la soluzione di compromesso sulla questione principale elaborata dalla Presidenza, che figura nella relazione.

Nuovo considerando, che fa parte della soluzione di compromesso:

«considerando che i dispositivi di verifica della firma devono assicurare che:

- i dati utilizzati per la verifica della firma corrispondano ai dati comunicati al verificatore;
- la firma sia verificata in modo affidabile e i risultati della verifica correttamente comunicati;

– il verificatore possa, all'occorrenza, stabilire in modo attendibile i contenuti dei dati usati per la firma;

– l'autenticità e validità del certificato necessario al momento della verifica della firma siano verificate in modo attendibile e che i risultati della verifica e dell'identità del firmatario siano comunicati correttamente e che l'uso di uno pseudonimo sia chiaramente indicato; e

– il verificatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.»

5.8.2 Proposta di direttiva sul commercio elettronico

Bruxelles, 18.11.1998
COM (1998) 586 def.
98/0325 (COD)

Proposta di direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti giuridici del commercio elettronico nel mercato interno (presentata dalla Commissione) – Sintesi.

I. OBIETTIVI

II. LA NECESSITÀ DI UN QUADRO GIURIDICO PER IL MERCATO INTERNO

1. La mancanza di chiarezza del quadro attuale
2. I costi economici elevati
3. Le conseguenze per gli investimenti e la competitività delle imprese europee
4. La mancanza di fiducia dei consumatori

III. LE QUESTIONI DA AFFRONTARE

1. Stabilimento degli operatori
2. Le comunicazioni commerciali
3. I contratti stipulati per via elettronica
4. La responsabilità degli intermediari
5. La composizione delle vertenze
6. Il ruolo delle autorità nazionali e il principio del paese d'origine

IV. APPROCCI

1. Trattare solo quanto strettamente necessario al mercato interno
2. Applicarsi a tutti i servizi della società dell'informazione
3. Affrontare le questioni all'interno di uno stesso strumento
4. Tralasciare gli aspetti esterni
5. Partire dai diritti e dalle libertà fondamentali
6. Istituire un quadro agile, flessibile, aperto all'evoluzione
7. Garantire un elevato livello di tutela dei consumatori

ALLEGATO: Commento articolo per articolo

PROPOSTA DI DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVA A TALUNI ASPETTI GIURIDICI DEL COMMERCIO ELETTRONICO NEL MERCATO INTERNO

CAPITOLO I - DISPOSIZIONI GENERALI

- Articolo 1 - Obiettivi e campo di applicazione
Articolo 2 - Definizioni
Articolo 3 - Mercato interno

CAPITOLO II - PRINCIPI

Sezione 1 - Regime di stabilimento e di informazione

- Articolo 4 - Superamento del principio di autorizzazione preventiva
Articolo 5 - Informazioni generali

Sezione 2 - Comunicazioni commerciali

Articolo 6 — Informazioni da fornire

Articolo 7 — Comunicazione commerciale non sollecitata

Articolo 8 — Professioni regolamentate

Sezione 3 Contratti per via elettronica

Articolo 9 — Trattamento dei contratti per via elettronica

Articolo 10 — Informazioni da fornire

Articolo 11 — Momento della conclusione del contratto

Sezione 4 Responsabilità degli intermediari

Articolo 12 — Semplice trasporto / «intermediario semplice»

Articolo 13 — «Caching»

Articolo 14 — Stoccaggio

Articolo 15 — Assenza dell'obbligo di sorveglianza

CAPITOLO III - ATTUAZIONE

Articolo 16 — Codici di condotta

Articolo 17 — Composizione extragiudiziale delle controversie

Articolo 18 — Ricorsi giurisdizionali

Articolo 19 — Cooperazione tra autorità

Articolo 20 — Vie elettroniche

Articolo 21 — Sanzioni

CAPITOLO IV- DEROGHE

Articolo 22 — Deroghe

CAPITOLO V - COMITATO CONSULTIVO E DISPOSIZIONI FINALI

Articolo 23 — Comitato

Articolo 24 — Trasposizione

Articolo 25 — Entrata in vigore

Articolo 26 — Destinatari

ALLEGATO I — (Attività escluse)

ALLEGATO II — (Deroghe all'articolo 3)

CAPITOLO IV ⁹⁹⁾**ESCLUSIONI DAL CAMPO DI APPLICAZIONE E DEROGHE****Art. 22*****Deroghe***

1. La presente direttiva non si applica:

- a) in materia tributaria,
- b) alla materia disciplinata dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio ¹⁰⁰⁾,
- c) alle attività dei servizi della società dell'informazione di cui all'allegato 1. L'elenco delle attività può essere modificato dalla Commissione secondo la procedura di cui all'articolo 23.

⁹⁹⁾ Si riportano i soli articoli di interesse per la presente Relazione.

¹⁰⁰⁾ GU L 281 del 23.11.1995, pag. 31.

2. L'articolo 3 non si applica alle materie di cui all'allegato II.

3. In deroga all'articolo 3, paragrafo 2 e fatte salve le azioni giudiziarie, le autorità competenti degli Stati membri possono limitare la libera circolazione di un servizio della società dell'informazione, rispettando il diritto comunitario e quanto segue:

a) le limitazioni devono:

(i) *essere necessarie per una delle seguenti ragioni:*

- ordine pubblico, come la tutela dei minori o la lotta contro l'incitamento all'odio razziale, sessuale, religioso od etnico,
- tutela della salute,
- pubblica sicurezza,
- tutela del consumatore;

(ii) *riguardare un servizio della società dell'informazione lesivo degli obiettivi di cui al punto (i) o che costituisca un rischio serio e grave di pregiudizio a tali obiettivi;*

(iii) *essere proporzionata a tali obiettivi.*

b) lo Stato membro deve aver preventivamente:

- chiesto allo Stato membro di cui all'articolo 3, paragrafo 1, di prendere provvedimenti senza reazioni da parte di quest'ultimo oppure senza che tali provvedimenti si siano rivelati sufficienti;
- notificato alla Commissione e allo Stato membro di stabilimento del prestatore la sua intenzione di prendere provvedimenti;

c) gli Stati membri possono prevedere nella loro legislazione che, in caso d'urgenza, non si applichino le condizioni di cui alla lettera b). I provvedimenti vanno allora immediatamente notificati alla Commissione e allo Stato membro di stabilimento del prestatore insieme ai motivi che fanno considerare urgente la situazione;

c) la Commissione può decidere della compatibilità con il diritto comunitario dei provvedimenti di limitazione. In caso di decisione negativa, lo Stato membro si asterrà dall'adottarli o sospenderà immediatamente quelli già adottati.

CAPITOLO V

COMITATO CONSULTIVO E DISPOSIZIONI FINALI

Art. 23

Comitato

La Commissione è assistita da un comitato a carattere consultivo, composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione.

Il rappresentante della Commissione sottopone al comitato un progetto delle misure da adottare. Il comitato, entro un termine che il presidente può fissare in funzione dell'urgenza della questione in esame, formula il suo parere sul progetto, eventualmente procedendo a votazione.

Il parere è iscritto a verbale: inoltre, ciascuno Stato membro ha il diritto di chiedere che la propria posizione figuri a verbale.

La Commissione tiene in massima considerazione il parere formulato dal comitato. Essa lo informa del modo in cui ha tenuto conto del suo parere.

Art. 24
Riesame

Entro tre anni dall'entrata in vigore della presente direttiva, e in seguito ogni due anni, la Commissione presenta al Parlamento europeo, al Consiglio e al Comitato economico e sociale una relazione sull'applicazione della presente direttiva, accompagnata, se necessario, da proposte per adeguarla all'evoluzione dei servizi della società dell'informazione.

5.9 AUTORITÀ DI CONTROLLO COMUNE SCHENGEN

5.9.1 Seconda relazione di attività dell'Autorità di controllo comune Schengen Marzo 1997 - Marzo 1998 (*)

BPh/CP

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 27 febbraio 1998
SCH/Aut-cont (98) 5, 2^a rev.
Traduzione: orig. FR

Indice

Prefazione

Capitolo I: INTRODUZIONE

Capitolo II: I COMPITI DELL'AUTORITÀ DI CONTROLLO COMUNE

Capitolo III: I TEMI TRATTATI

Capitolo IV: I PARERI DELL'AUTORITÀ DI CONTROLLO COMUNE

Capitolo V: PROGRAMMA D'AZIONE DELL'AUTORITÀ DI CONTROLLO COMUNE

Allegati ¹⁰¹⁾

Cenni storici

Organi comuni preposti all'applicazione della Convenzione

Obiettivo ed architettura del SIS

Gli uffici SIRENE

Protezione dei dati personali

Organigramma dei gruppi di lavoro Schengen

Pareri dell'Autorità di controllo comune

Regolamento interno dell'Autorità di controllo comune

Membri dell'Autorità di controllo comune

Diritto di accesso e di comunicazione al cittadino delle informazioni contenute nel Sistema d'informazione Schengen che lo riguardano.

PREFAZIONE

Il periodo coperto dalla seconda relazione annuale dell'Autorità di controllo comune Schengen (marzo 1997-marzo 1998) è un periodo decisivo e di cruciale importanza per la cooperazione di polizia e per il Sistema di informazione Schengen sul piano europeo: allargamento a nuovi Paesi delle condizioni per l'esercizio della libertà di circolazione dei cittadini, rafforzamento del sistema comune di sicurezza e di informazione di polizia ed integrazione di Schengen nell'Unione europea.

(*) Si riproduce il testo nella traduzione curata dal Segretariato dell'ACC.

¹⁰¹⁾ Gli Allegati non sono riportati nella presente Relazione, ma sono disponibili presso gli uffici del Garante.

Il 1997 ha visto affermarsi l'indipendenza e l'importanza delle attività dell'Autorità di controllo comune (ACC) quale organo incaricato di vigilare al rispetto dei diritti e delle libertà dei cittadini, in particolare per quanto riguarda la protezione dei dati di natura personale.

L'ACC ha avuto modo di intervenire in questioni fondamentali, contribuendo positivamente ad un funzionamento del Sistema d'informazione Schengen rispettoso delle regole e dei diritti previsti dalla Convenzione di applicazione. In questa prospettiva vanno visti l'analisi delle leggi sulla protezione dei dati di Italia e Grecia, le raccomandazioni ed i pareri relativi alle condizioni di sicurezza nel trattamento e nella trasmissione delle informazioni di natura personale, alla durata di conservazione dei dati, alle segnalazioni relative a dati di identità usurpati e alla trasmissione di determinati dati ad Interpol.

L'ACC ha visto riconoscere il suo ruolo rilevante da parte degli organi esecutivi di Schengen: ha ricevuto una dotazione finanziaria grazie ad una linea di bilancio autonoma, ha ricevuto con maggiore regolarità le informazioni indispensabili ai fini dell'esercizio dei suoi compiti ed è stata invitata a formulare pareri su diverse materie. Le successive presidenze Schengen (Portogallo, Austria e Belgio) hanno riconosciuto sempre maggiore importanza all'ACC.

In adempimento al suo programma di lavoro, l'ACC ha compiuto nel corso dell'anno passi determinanti ai fini del funzionamento trasparente del sistema e dell'informazione dei cittadini. In occasione della conferenza stampa tenutasi a Lisbona nel mese di aprile 1997, l'ACC ha reso pubblica la sua relazione precedente e l'ha in seguito comunicata alle autorità europee e agli organi Schengen. Le autorità di controllo nazionali ne hanno successivamente informato i rispettivi parlamenti. Questo bilancio delle attività ha beneficiato di diverse pubblicazioni ed è oggi disponibile sui siti Internet delle autorità di controllo nazionali. L'ACC ha inoltre richiamato l'attenzione delle autorità competenti e dell'opinione pubblica per porre in evidenza i problemi di sicurezza derivanti dalla fuga di informazioni verificate presso un ufficio SIRENE. Ha altresì deciso di varare, di concerto con le autorità nazionali competenti, una campagna di informazione sui diritti del cittadino.

Nell'ambito dell'evoluzione dei sistemi di informazione di polizia europei (Europol, Eurodac, Sistema d'informazione doganale) e dell'intensificazione delle misure di cooperazione nella lotta alla grande criminalità organizzata, vanno approfonditi i meccanismi di collaborazione tra le autorità di controllo comuni incaricate, nel quadro di tali sistemi di informazione, di salvaguardare i valori fondamentali della libertà e della cittadinanza. L'ACC tenderà di stimolare questa collaborazione avvalendosi, come avvenuto in passato, del sostegno attivo delle autorità di controllo nazionali.

L'integrazione di Schengen nell'Unione europea, prevista dal Trattato di Amsterdam, rappresenterà un plusvalore per la trasparenza di Schengen. Il patrimonio legislativo europeo si arricchirà grazie alle disposizioni della Convenzione di Schengen relative ai diritti in materia di protezione dei dati personali. L'incorporazione dell'acquis di Schengen nell'Unione europea comprenderà necessariamente le principali raccomandazioni dell'ACC nonché il ruolo che questa sarà chiamata a svolgere.

L'ACC pianificherà le sue azioni e compierà il massimo sforzo per affermare uno spazio europeo comune di libertà e di sicurezza.

Marzo 1998

Il Presidente JOÃO LABESCAT

Capitolo I

INTRODUZIONE

Nella sua prima relazione, l'Autorità di controllo comune ha richiamato il percorso dei cinque Stati firmatari dell'Accordo di Schengen dal 1985 sino alla firma della Convenzione di applicazione del 1990 e, più tardi, alla messa in applicazione di tale Convenzione nel marzo 1995. Ha inoltre illustrato come, nell'arco di questo periodo, ai cinque Stati firmatari si siano aggiunti dieci nuovi Paesi, anch'essi desiderosi di far parte di uno spazio di libera circolazione delle persone ¹⁰²⁾.

L'ACC ha inoltre descritto le misure compensative previste dalla Convenzione di applicazione dell'Accordo di Schengen per conseguire l'obiettivo dell'abolizione dei controlli alle frontiere interne degli Stati membri e, di conseguenza, della creazione di un grande spazio di libera circolazione delle persone all'interno del quale il livello di sicurezza sia almeno pari a quello esistente in precedenza. Tali misure compensative sono brevemente descritte qui di seguito.

Tra le misure compensative all'abolizione dei controlli alle frontiere interne previste dalla Convenzione figura, oltre all'armonizzazione della politica in materia di rilascio dei visti, alla politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, al miglioramento della cooperazione di polizia e giudiziaria, all'intensificazione della lotta al traffico illecito di stupefacenti e all'armonizzazione del livello dei controlli alle frontiere esterne dello spazio Schengen, anche il Sistema di informazione Schengen (SIS).

Si tratta di un sistema che collega i Paesi che applicano la Convenzione di applicazione dell'Accordo di Schengen e consente ai suoi utenti (servizi di polizia, ambasciate, consolati, ...) di disporre in tempo reale di informazioni utili ai fini dell'esercizio dei loro compiti, inserite da qualsiasi Stato che applica la Convenzione.

Tali informazioni riguardano le persone (ricercate per l'arresto ai fini dell'estradizione, non ammissibili, scomparse, oggetto di sorveglianza discreta, ...) o gli oggetti (veicoli, armi, banconote o documenti rubati, sottratti o smarriti). La creazione di questo strumento è stata accompagnata dall'istituzione di un'Autorità di controllo comune per la protezione dei dati di natura personale (ACC) incaricata, in particolare, di vigilare al rispetto delle disposizioni della Convenzione da parte dell'unità di supporto tecnico del SIS (art. 115). L'ACC, composta di due rappresentanti dell'autorità di controllo di ciascuna Parte contraente, si è inoltre vista affidare un ruolo di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

Dalla messa in applicazione della Convenzione, l'ACC ha avuto molte difficoltà a far riconoscere la propria competenza e la propria indipendenza dagli organi esecutivi di Schengen. Questa situazione è chiaramente illustrata nella prima relazione, nella quale vengono sottolineate, in particolare, le difficoltà

¹⁰²⁾ Fanno parte dell'ACC: Belgio, Lussemburgo, Paesi Bassi, Francia, Germania, Italia, Spagna, Portogallo, Grecia e Austria. I cinque Stati nordici (Svezia, Finlandia, Danimarca, Norvegia e Islanda) partecipano ai lavori dell'ACC nella qualità di osservatori.

per ottenere un bilancio autonomo e le difficoltà con cui si è imbattuto gruppo di esperti incaricato dall'ACC di effettuare una visita di controllo presso la sezione centrale del SIS (il C.SIS) a Strasburgo.

Nonostante i progressi realizzati, il cammino da percorrere è ancora lungo. La visita di controllo al C.SIS effettuata nel 1996 ha dimostrato un corretto funzionamento globale del sistema ma ha anche posto in evidenza diverse difficoltà, alcune delle quali creano veri e propri problemi in termini di integrità dei dati.

I problemi evidenziati dall'ACC assumono una particolare rilevanza in un momento in cui si assiste ad un aumento del numero di Stati Schengen che applicano la Convenzione passati, alla fine del 1997, da sette a dieci ed al conseguente aumento del volume di dati inseriti nel SIS.

Come tutti i sistemi di informazione di polizia, anche il sistema Schengen è in fase di evoluzione, evoluzione che deve essere accompagnata da un aumento dell'importanza del ruolo delle autorità di controllo indipendenti. L'integrazione di Schengen nell'Unione europea, prevista all'art. 7 del Protocollo sull'integrazione dell'acquis di Schengen del Trattato di Amsterdam, vuol dire maggiore trasparenza e maggiori garanzie per i diritti fondamentali del cittadino. I parlamenti nazionali e gli organi europei svolgeranno un ruolo attivo nel conseguimento di questi obiettivi

Capitolo II

COMPITI DELL'AUTORITÀ DI CONTROLLO COMUNE

Sebbene il suo compito principale consista nel controllo dell'unità di supporto tecnico del SIS, compito che è la sola a poter esercitare (art. 115, 2 comma), all'ACC è altresì attribuito un ruolo di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

La Convenzione di applicazione dell'Accordo di Schengen ne precisa i compiti nei seguenti articoli.

Articolo 106, 3° comma:

– l'ACC formula un parere in caso di disaccordo tra due Parti contraenti in merito all'esistenza di un errore di diritto o di fatto in una segnalazione. In tal caso, l'ACC deve essere obbligatoriamente adita dalla Parte contraente che non è all'origine della segnalazione.

Articolo 115, 3° comma:

- l'ACC analizza le difficoltà di applicazione o di interpretazione che possono sorgere nell'utilizzo del SIS;
- l'ACC esamina i problemi che possono sorgere durante il controllo indipendente effettuato dalle autorità di controllo nazionali delle Parti contraenti;
- l'ACC esamina i problemi che possono porsi nell'esercizio del diritto di accesso al sistema;
- su un piano più generale, l'ACC elabora proposte armonizzate allo scopo di trovare soluzioni ai problemi esistenti.

Articolo 115, 4° comma:

– l'ACC elabora relazioni che vengono trasmesse alle autorità alle quali pervengono le relazioni delle autorità di controllo nazionali.

Articolo 118, 2° comma:

– l'ACC viene informata delle misure particolari adottate da ogni Parte contraente per assicurare la protezione dei dati in occasione della loro trasmissione a servizi situati al di fuori del territorio delle Parti contraenti.

Per quanto riguarda gli scambi di informazioni non riguardanti il SIS:

Articolo 126, 3° comma, lettera f):

– l'ACC può, su richiesta delle Parti contraenti, formulare un parere sulle difficoltà di applicazione e di interpretazione dell'art. 126 relativo al trattamento dei dati trasmessi, al di fuori del SIS, in applicazione della Convenzione.

Articolo 127, 1° comma:

– l'ACC può, alle condizioni e secondo le modalità previste all'art. 126, formulare un parere in caso di trasmissione di dati provenienti da un archivio non automatizzato e di inserimento di dati in un tale archivio.

Capitolo III

I TEMI TRATTATI

Dal mese di marzo 1997 al mese di marzo 1998, l'ACC si è riunita dieci volte in sessione plenaria. Ad eccezione della sessione annuale tenutasi a Lisbona in aprile 1997, alla quale ha preso parte il Presidente del Comitato esecutivo, tutte le riunioni si sono svolte a Bruxelles. Oltre alle riunioni plenarie, l'ACC ha organizzato tre riunioni in cerchia ristretta destinate a preparare i progetti di «Parere» su problemi specifici. L'Autorità, rappresentata da alcuni dei suoi membri, ha inoltre incontrato in tre occasioni i rappresentanti del Ministero dell'Interno francese, responsabile dell'unità di supporto tecnico del C.SIS. Ad uno di questi incontri ha preso parte anche la Troika Schengen per fare il punto, in particolare, sull'applicazione delle raccomandazioni formulate dall'ACC dopo la visita di controllo al C.SIS.

Va sottolineato che, in conformità della decisione presa dall'ACC il 10 e l'11 febbraio 1997 a Strasburgo, dalla riunione del 7 marzo 1997 partecipano ai lavori nella qualità di osservatori anche i rappresentanti di Svezia, Danimarca, Finlandia, Norvegia ed Islanda.

Nel corso delle varie riunioni sono state affrontate le seguenti tematiche:

Pareri dell'ACC

L'ACC ha adottato una serie di pareri relativi a temi specifici (v. Capitolo IV).

Composizione dell'ACC

L'ACC ha preso atto dell'esistenza delle leggi italiana e greca che disciplinano la protezione dei dati di natura personale. Si trattava infatti di una delle condizioni preliminari per il caricamento dei dati personali nel SIS (art. 117) e, di conseguenza, per la messa in applicazione della Convenzione in questi Stati membri. L'ACC ha adattato il proprio regolamento interno¹⁰³⁾ al fine di poter attribuire lo status di membri dell'ACC ai rappresentanti delle autorità di controllo nazionali degli Stati che hanno aderito alla Convenzione dal momento in cui,

¹⁰³⁾ Il documento è allegato alla presente relazione.

avendo soddisfatto tutte le altre condizioni, la Convenzione viene messa in applicazione nei loro Paesi. In virtù di questo criterio, i rappresentanti delle autorità di controllo di Italia, Grecia ed Austria si sono visti riconoscere lo status di membri a pieno titolo dell'ACC in occasione della riunione del 12 dicembre 1997.

Linea di bilancio autonoma per l'ACC

Al termine di lunghe discussioni di principio, le autorità Schengen hanno approvato il bilancio dell'ACC per il 1997. La versione approvata dal Comitato esecutivo il 25 aprile 1997 è stata successivamente adattata a seguito dell'aumento del numero di Paesi partecipanti alle riunioni. Il bilancio attribuito all'ACC per il 1997 ammonta a 2.839.950 BEF. Il 12 dicembre 1997 l'ACC ha proceduto alla chiusura dei conti 1997 dalla quale risulta un saldo attivo di 992.179 BEF. Le spese sostenute durante l'anno riguardavano la realizzazione dell'opuscolo sul diritto di accesso, l'elaborazione, la traduzione e la stampa della prima relazione di attività, l'organizzazione della sessione annuale a Lisbona e l'acquisto di materiale. Il bilancio del 1998 elaborato tenendo conto delle spese sostenute nel 1997 e del programma di attività del 1998, ammonta a 3.239.950 BEF ed è stato approvato dal Gruppo centrale il 23 febbraio 1998.

Controllo del C.SIS

La versione definitiva della relazione tecnica riservata sulla visita di controllo al C.SIS, contenente le reazioni del Ministero dell'Interno francese, è stata approvata. La versione provvisoria della relazione era stata comunicata al Presidente del Gruppo centrale nel dicembre 1996, mentre la versione definitiva è stata sottoposta il 22 aprile 1997 al Presidente del Comitato esecutivo e al Presidente del Gruppo centrale perché provvedessero alla sua diffusione ai gruppi tecnici competenti. Questi sono stati incaricati di verificare la possibilità di implementare le raccomandazioni formulate dall'ACC per aumentare il livello di sicurezza del sistema. Le prime risposte sono state presentate il 4 marzo 1998, in occasione di una riunione del Gruppo centrale appositamente dedicata al SIS, alla quale ha preso parte una delegazione dell'ACC. Questa esaminerà le risposte in occasione delle sue future riunioni.

Relazione di attività

L'ACC ha elaborato la sua prima relazione di attività. Il primo progetto risale al 7 marzo mentre la versione definitiva è stata approvata il 27 marzo 1997. La struttura della seconda relazione è stata concordata il 3 febbraio 1998. Il progetto di testo è stato sottoposto a discussione il 25 febbraio nel quadro di un comitato di redazione ristretto e successivamente approvato in sessione plenaria il 6 marzo 1998.

Conferenza stampa dell'ACC

L'ACC ha organizzato una sessione annuale il 22 e il 23 aprile 1997 a Lisbona. La relazione di attività è stata presentata al Presidente del Gruppo centrale e ai giornalisti che hanno assistito alla conferenza stampa.

A questa hanno preso parte numerosi giornalisti della televisione, della radio, dei principali quotidiani e delle agenzie di stampa portoghesi nonché giornalisti stranieri, in particolare delle agenzie di stampa spagnola (EFE) e britannica (Reuters). La riunione e la presentazione della relazione dell'ACC hanno beneficiato di grande eco nella stampa e di articoli in diversi periodici.

Le tematiche che hanno maggiormente suscitato l'attenzione dei mass media sono state la definizione delle competenze dell'ACC, il suo ruolo nel quadro della struttura Schengen, il funzionamento del SIS (contenuto, tipo di dati e forme di accesso) nonché le informazioni generali sulla Convenzione di applicazione dell'Accordo di Schengen.

Relazioni dell'ACC con gli organi Schengen

Il 16 giugno 1997 si è tenuta a Bruxelles una riunione tra i rappresentanti dell'ACC, del Gruppo centrale e del Ministero dell'Interno francese nella sua qualità di responsabile dell'unità di supporto tecnico C.SIS. I rappresentanti dell'ACC sono stati informati dello stato di avanzamento delle attività relative al caricamento dei dati reali di Italia, Grecia ed Austria nel SIS. Sono state inoltre fornite informazioni in merito alla capacità da parte del SIS di accogliere i tre nuovi Paesi. È stata evocata la questione del seguito da dare alla relazione riservata sulla visita di controllo al C.SIS e i partecipanti alla riunione hanno approvato la proposta del Ministero dell'Interno francese di elaborare, di concerto con i rappresentanti dell'ACC, un protocollo che definisca le modalità delle future visite di controllo presso il C.SIS.

Sono state precisate le modalità di utilizzo del bilancio dell'ACC ed è stato ufficialmente presentato il parere 97/1 sulla duplicazione di una parte delle segnalazioni del SIS.

È stato concordato il principio di incontri periodici tra i rappresentanti dell'ACC e del Gruppo centrale, eventualmente a margine delle riunioni di quest'ultimo. Questi incontri hanno offerto lo spunto per migliorare lo scambio di informazioni tra le due autorità

Segretariato dell'ACC

In diverse occasioni e in particolare nell'incontro evocato nel paragrafo precedente, l'ACC ha sollecitato un rafforzamento dei mezzi logistici messi a sua disposizione e chiesto di usufruire di una priorità nelle traduzioni rispetto agli altri gruppi di lavoro. Ha inoltre pregato che venga esaminata la possibilità di disporre di un segretariato autonomo. Troppo spesso, infatti, l'aumento del numero delle riunioni dei gruppi di lavoro Schengen pregiudica la preparazione delle riunioni dell'ACC. Questa ha inoltre constatato che il personale del Segretariato generale viene prioritariamente assegnato alla preparazione delle riunioni del Gruppo centrale e del Comitato esecutivo. Il problema è stato parzialmente risolto grazie all'attribuzione di un bilancio all'ACC che consente, tra l'altro, di coprire le spese di traduzione della relazione annuale. Il 23 febbraio 1998 il Gruppo centrale ha approvato il rafforzamento dello staff messo a disposizione dell'ACC. Questa se ne rallegra in quanto ritiene che sarà in grado di far fronte alla crescente mole di lavoro solo potendosi avvalere di un segretariato permanente o, quanto meno, assegnato prioritariamente alle sue attività. L'ACC considera inoltre che nessuno meglio del segretariato attuale, che ha accompagnato le sue attività sin dall'elaborazione della Convenzione, sarà in grado di fornire tale sostegno amministrativo.

Modalità delle visite di controllo al C.SIS

Nel corso dell'anno è stato esaminato il protocollo destinato a precisare le modalità di realizzazione delle future visite di controllo al C.SIS. Poiché in occasione della riunione del 12 dicembre 1997 la maggior parte delle delegazioni dell'ACC ha considerato che il progetto sul quale erano sfociati i vari incontri tra i rappresentanti del Ministero dell'Interno francese e i rappresentanti dell'ACC

non riconosceva il carattere indipendente di quest'ultima, è stato concordato di affidare l'esame di questa delicata questione ad un gruppo ristretto incaricato di presentare un nuovo progetto che concili le esigenze di sicurezza poste dal Ministero dell'Interno francese e la necessità di consentire all'ACC di effettuare i controlli in piena indipendenza. Il nuovo progetto è stato elaborato dal gruppo ristretto dell'ACC il 2 febbraio 1998 ed approvato in sessione plenaria il 6 marzo 1998. Il documento fungerà da nuova base di discussione con le autorità competenti.

Informazione dell'ACC

Su richiesta dell'ACC, nel mese di aprile 1997, il Gruppo centrale ha invitato il C.SIS e l'Unità di gestione a mettere a disposizione le loro relazioni mensili. L'ACC considerava infatti necessario disporre di tali documenti per accertare che vengano rispettate le regole in materia di protezione dei dati personali.

Il 7 maggio 1997, il Presidente del Gruppo centrale ha inviato una lettera al Presidente del Gruppo di lavoro permanente e al capo delegazione francese responsabile del C.SIS invitandoli a dare esecuzione alla decisione del Gruppo centrale. Se nel frattempo il C.SIS ha regolarmente trasmesso le sue relazioni all'ACC, questa non ha al momento ricevuto copia di alcun documento dell'Unità di gestione.

Trasparenza nei confronti del cittadino

Per adempiere alla propria missione di informazione nei confronti del cittadino, l'ACC aveva deciso di pubblicare un opuscolo esplicativo sul diritto di accesso ai dati da parte delle persone segnalate nel SIS. Il 12 dicembre 1997, l'ACC ha adottato la versione definitiva del testo esplicativo sul diritto di accesso dei cittadini ai dati SIS che li riguardano, al quale sono allegati gli estremi delle autorità nazionali. Il testo, allegato alla presente relazione, sarà distribuito presso i valichi autorizzati delle frontiere esterne Schengen sotto forma di opuscolo e di locandine informative. Tale diffusione sarà possibile solo con l'ausilio delle autorità di controllo nazionali e del Gruppo centrale.

Sicurezza degli uffici SIRENE

A seguito della scoperta di un traffico di informazioni sensibili, in particolare provenienti dal SIS, presso l'ufficio SIRENE belga¹⁰⁴⁾, l'ACC, immediatamente messa al corrente dell'accaduto, ha adottato, il 12 dicembre 1997, un comunicato stampa, diffuso lo stesso giorno alle agenzie di stampa e comunicato il 15 dicembre 1997 al Comitato esecutivo.

Nel suo comunicato stampa, l'ACC esprime viva preoccupazione per questo incidente che ha posto drammaticamente in evidenza la necessità di migliorare costantemente le misure di sicurezza nell'ambito del SIS e dello scambio di informazioni Schengen.

L'ACC ha invitato le autorità di controllo nazionali a:

- riferire senza indugio all'ACC sulla situazione specifica in materia di sicurezza nella rispettiva sezione del SIS e nel rispettivo ufficio SIRENE;
- determinare, sulla base di tali relazioni, le misure che dovrebbero essere adottate al fine di migliorare la sicurezza;

¹⁰⁴⁾ La descrizione delle funzioni degli uffici SIRENE figura in allegato.

- valutare la necessità di una relazione annuale sulla situazione in materia di sicurezza;
- riferire sulla questione in occasione della prossima riunione.

L'ACC ha inoltre sottolineato l'importanza di essere mantenuta al corrente delle misure di sicurezza adottate dagli organi Schengen e dalle autorità nazionali, al fine di garantire la riservatezza del Sistema d'Informazione Schengen.

Da quella data diverse autorità di controllo nazionali hanno proceduto a delle verifiche. L'esame delle prime relazioni nazionali è attualmente in corso.

Elezione del Presidente e del Vicepresidente

Il 12 dicembre 1997 e il 3 febbraio 1998, i sigg. J. Labescat (Portogallo) e B. De Schutter (Belgio) sono stati eletti rispettivamente Presidente e Vicepresidente dell'ACC.

Capitolo IV

I PARERI DELL'AUTORITÀ DI CONTROLLO COMUNE

Nel riesaminare i vari pareri formulati, l'ACC ha rilevato che alcuni di essi richiedevano precisazioni supplementari. Per questo motivo, alcuni dei pareri illustrati in appresso erano già citati tra le attività in corso nella prima relazione di attività. I primi due pareri, approvati in marzo 1997, figuravano inoltre nella prima relazione dell'ACC. Si presenta di seguito un sunto dei vari pareri la cui versione integrale figura in allegato.

1. Parere del 7 marzo 1997 sul progetto pilota del Gruppo di lavoro I «Polizia e sicurezza» relativo agli itinerari dei veicoli rubati (doc. SCH/Aut-cont (97) 22 riv.)

Il 10 febbraio 1997, il Gruppo centrale ha trasmesso all'ACC una domanda di parere emanante dal Gruppo di lavoro I «Polizia e sicurezza» relativa alla partecipazione dei Paesi non integrati nel SIS ad un progetto pilota in materia di veicoli rubati.

Dopo aver preso conoscenza del fatto che il progetto intendeva consentire ai Paesi non integrati nel SIS di consultare il sistema per il tramite dei loro funzionari di collegamento, l'ACC ha chiesto informazioni supplementari in merito al tipo di informazioni scambiate e alle modalità di trasmissione.

Una volta ricevute le informazioni richieste, il 7 marzo 1997 l'ACC ha formulato un parere nel quale ribadisce che:

- le informazioni relative alla marca, al tipo, al colore e alle caratteristiche tecniche del veicolo non sono, di per sé, dati di natura personale a condizione che non siano associati alla targa, al proprietario o al conducente del veicolo in causa;

- gli scambi di informazioni di polizia provenienti dagli archivi nazionali tra le Parti contraenti integrate nel SIS e gli altri Stati nei quali la Convenzione non è stata ancora messa in applicazione sono retti dai meccanismi della cooperazione bilaterale o multilaterale e assoggettati alle disposizioni delle legislazioni sulla protezione dei dati e alla verifica delle autorità di controllo nazionali.

L'ACC ha considerato che, in conformità degli articoli 101 e 126, 1° comma della Convenzione, i dati direttamente o indirettamente personali inseriti nel SIS non sono accessibili né possono essere consultati direttamente dalle autorità delle Parti contraenti nel territorio delle quali la Convenzione non è ancora stata messa in applicazione.

Il parere è stato comunicato al Gruppo di lavoro I che lo ha preso in considerazione nell'esecuzione del progetto pilota. Anche gli altri progetti pilota, e in particolare quello attualmente in preparazione sugli itinerari del traffico di stupefacenti, dovranno tener conto di tale parere.

2. Parere del 7 marzo 1997 sul progetto di accordo di cooperazione in materia di contestazione delle infrazioni stradali e di esecuzione delle sanzioni pecuniarie (doc. SCH/Aut-cont (97) 19 riv.)

Il 10 febbraio 1997, il Gruppo centrale ha trasmesso all'ACC una domanda di parere proveniente dal Gruppo di lavoro III «Cooperazione giudiziaria» relativo ad un progetto di accordo sulle infrazioni stradali.

Il testo prevede un accesso alle informazioni e ai dati che figurano nei registri dell'Ufficio della motorizzazione delle Parti contraenti, un sistema di comunicazione diretta e di cooperazione nonché, con riserva di taluni casi nei quali l'applicazione della sanzione pecuniaria è limitata o esclusa, l'esecuzione effettiva ad opera delle autorità di un paese delle decisioni dell'autorità di un'altra Parte contraente.

Il progetto di accordo si fonda sulla dichiarazione comune dei Ministri e Segretari di Stato del 19 giugno 1990, ai sensi della quale le Parti contraenti si impegnano ad avviare o proseguire le discussioni in diversi settori tra cui i procedimenti per infrazioni in materia di circolazione stradale e l'esecuzione reciproca delle pene pecuniarie.

Si tratta di uno strumento giuridico internazionale distinto ma complementare della Convenzione di Schengen che, nel suo Titolo VI, fa esplicito riferimento alle regole di protezione dei dati applicabili in caso di trasmissione di informazioni non inserite nel SIS.

Dopo aver esaminato le disposizioni in materia di protezione dei dati previste dal progetto di accordo, il 27 marzo 1997 l'ACC ha formulato un parere nel quale considera che questo debba integrare o esplicitare i seguenti principi:

- il diritto di qualsiasi persona di esigere la rettifica o la cancellazione di dati che la riguardano contenenti errori di diritto o di fatto;
- il principio di cooperazione tra le autorità di controllo nazionali di cui all'art. 128, 1° comma, al fine di garantire i diritti di accesso, di rettifica o di cancellazione;
- la competenza dell'ACC per formulare pareri riguardo agli aspetti comuni, in materia di protezione dei dati personali, derivanti dall'applicazione dell'accordo.

Il parere è stato trasmesso al Gruppo di lavoro III che ha adattato il progetto in conformità.

3. Parere 97/1 del 22 maggio 1997 sulla duplicazione di una parte delle segnalazioni dei SIS (doc. SCH/Aut-cont (97) 38)

L'art. 102, 2° comma della Convenzione dispone che i dati inseriti nel SIS «possono essere duplicati soltanto per fini tecnici, sempre che l'operazione sia necessaria per la consultazione diretta da parte delle autorità» abilitate.

Su richiesta dell'Autorità di controllo nazionale belga, l'ACC ha avviato una riflessione su questo articolo volta ad interpretare i concetti di «duplicazione per fini tecnici» e di «consultazione diretta» in particolare alla luce della proce-

dura di interrogazione automatizzata di cui all'art. 92 della Convenzione. Ha inoltre valutato le conseguenze di una duplicazione su CD-ROM dell'integralità o di una parte di una base dati N.SIS ai fini di una consultazione ad opera, in particolare, delle rappresentanze diplomatiche o consolari.

L'esame delle condizioni di applicazione dell'art. 102, 2° comma ha suscitato quesiti relativi all'aggiornamento delle informazioni duplicate e alla sicurezza delle trasmissioni effettuate verso uffici situati al di fuori del territorio delle Parti contraenti.

L'ACC ha pertanto proposto una soluzione armonizzata compatibile con le regole di protezione dei dati stabilite dalla Convenzione.

Nel suo parere 97/1, l'ACC ricorda che, a prescindere dai mezzi determinati dagli Stati per organizzare la consultazione delle segnalazioni ex art. 96 della Convenzione da parte delle rispettive rappresentanze diplomatiche e consolari, vanno rispettati i seguenti principi della Convenzione:

- le tecniche e i mezzi di duplicazione devono garantire l'identità di dati in tempo reale rispetto al trattamento centrale SIS;
- tali tecniche e mezzi devono garantire il livello minimo di protezione previsto all'art. 118, 1 comma e più in particolare alle lettere *b*), *d*) e *f*) di tale articolo; nonché conformarsi al disposto dell'art. 118, 3 comma;
- il programma che consente la loro utilizzazione deve permettere una registrazione che soddisfa il disposto dell'art. 103.

Tali registrazioni devono essere rimpatriate ogni sei mesi ed essere tenute a disposizione dell'autorità di controllo nazionale di cui all'art. 114 della Convenzione presso l'autorità che ha la competenza centrale per la sezione nazionale del SIS ai sensi dell'art. 108, 1 comma.

In caso di utilizzazione dei mezzi di duplicazione che presentano un rischio in materia di identità di dati, l'ACC raccomanda insistentemente che la Parte contraente che assume in tal modo la sua responsabilità, come prevista dagli articoli 92, 2° comma e 116, sia tenuta:

- in caso di segnalazione della persona nel supporto di duplicazione utilizzato, ad effettuare una verifica in tempo reale (rete, telefono, fax) per accertarsi della conferma di tale informazione;
- in caso di non segnalazione della persona nel supporto di duplicazione utilizzato, ad accettare la propria responsabilità in caso di segnalazione di questa stessa persona intervenuta nel lasso di tempo tra l'incisione dei dati sul supporto di duplicazione e il tempo reale. Questa responsabilità può venir meno solo mediante la prova di una verifica in tempo reale effettuata al momento della domanda di visto.

Nell'esaminare la problematica, l'ACC ha osservato che, contrariamente alle disposizioni dell'art. 118, 2 comma, non era stata informata delle misure particolari prese da ciascuna Parte contraente per garantire la sicurezza dei dati in occasione della loro trasmissione a servizi situati al di fuori del loro territorio.

Il 6 dicembre 1996, l'ACC ha pertanto chiesto al Gruppo centrale di precisare in che modo ogni Stato Schengen applica il disposto dell'art. 118, 2° comma. Sulla base delle risposte ricevute il 4 marzo 1998, l'ACC verificherà se le misure applicate sono conformi alla sua interpretazione di questa disposizione della Convenzione.

4. *Parere 98/1 del 3 febbraio 1998 sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione (doc. SCH/Aut-cont (97) 55, 2^a rev.)*

L'attenzione dell'ACC è stata richiamata sulle difficoltà poste, alla luce dell'art. 102, 1° comma della Convenzione, dalla conservazione dei dossier relativi alle segnalazioni dopo la cancellazione delle stesse.

L'art. 102, 1° comma vieta infatti alle Parti contraenti di utilizzare i dati ex artt. 95-100 per fini diversi da quelli enunciati per ciascuna delle segnalazioni.

I servizi di polizia nazionali di determinate Parti contraenti continuano tuttavia a conservare i dossier anche ad avvenuta cancellazione di segnalazioni ex art. 95 e segg. della Convenzione e ne fanno l'oggetto di fascicoli penali

Le autorità di polizia interessate si basano, in tale contesto, sulle disposizioni previste dal diritto nazionale (cfr. punto 2.1.3, lett b) del Manuale SIRENE) e sulle disposizioni di cui al Titolo VI della Convenzione di Schengen.

L'ACC ha considerato che si tratta di una questione estremamente importante alla luce del principio della finalità dei dati. Nel suo parere del 3 febbraio 1998, conferma i principi ed i diritti fondamentali in materia di protezione dei dati di cui alla Convenzione di Schengen, in particolare:

a) i dati del SIS possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (artt. 102, 1° comma e 94, 1° comma). Una deroga a tale principio generale è ammessa soltanto se giustificata dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la sicurezza pubblica dello Stato, per gravi ragioni di sicurezza dello Stato o ai fini della prevenzione di un fatto punibile grave (art. 102, 3° comma);

b) qualsiasi utilizzo dei dati non conforme ai commi da 1 a 4 dell'art. 102 sarà considerato uno sviamento di finalità (art 102, 5° comma);

c) in conformità dell'art. 112, i dati personali inseriti nel Sistema d'Informazione Schengen ai fini della ricerca di persone sono conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti;

d) questi principi si applicano, nel quadro di un'interpretazione integrativa della Convenzione, a ogni tipo di trattamento dell'informazione relativo a segnalazioni contenute nel Sistema d'Informazione Schengen o basato sulle stesse.

L'Autorità di controllo comune considera pertanto che si debbano adottare le seguenti misure:

a) in caso di soppressione di una segnalazione ai fini della ricerca di persone, ciascuna Parte contraente Schengen, in conformità dell'art. 112 della Convenzione, è tenuta a cancellare tale segnalazione e a distruggere senza indugio la corrispondente documentazione;

b) le autorità Schengen devono procedere ad una revisione del Manuale SIRENE allo scopo di cancellare le disposizioni del punto 21.3 lettera b), contrarie alle disposizioni della Convenzione.

5. *Parere 98/2 del 3 febbraio 1998 sull'usurpazione di identità e sulle conseguenze di una segnalazione SIS per il titolare legittimo di un'identità usurpata (doc. SCH/Aut-cont (97) 42, 2^a rev.)*

In alcuni Paesi, in caso di usurpazione di identità l'autore dell'usurpazione viene segnalato nel SIS sotto il nome della persona la cui identità è stata usurpata.

In altre parole, il sistema contiene una segnalazione relativa ad un'identità che non corrisponde né di fatto né di diritto all'identità reale della persona ricercata. La persona vittima di un'usurpazione di identità si trova così segnalata nel SIS senza esserne stata preliminarmente informata.

Taluni Stati ritengono che in tali circostanze sia necessario procedere immediatamente alla cancellazione dei dati relativi alla vittima dell'usurpazione di identità. Altri considerano invece che la segnalazione relativa all'identità usurpata vada mantenuta nel SIS anche se la persona indebitamente segnalata ne chiede la cancellazione. L'argomento addotto a favore della conservazione della segnalazione è la necessità di ricercare l'autore dell'usurpazione.

L'ACC ha esaminato i problemi posti dall'utilizzazione abusiva di alias di persone segnalate nel SIS alla luce dei principi di protezione dei dati di natura personale previsti dalla Convenzione di Schengen ed ha riaffermato, in particolare, i seguenti principi e diritti fondamentali in materia di protezione dei dati:

a) i dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (art. 102, 1° comma e art. 94, 1° comma). Si tratta di un principio generale a cui si può derogare in via eccezionale se necessario per prevenire una minaccia grave o un reato grave (art. 102, 3° comma).

b) qualunque utilizzazione dei dati non conforme ai commi da 1 a 4 dell'art. 102 sarà considerata uno sviamento di finalità (art. 102, 5° comma).

c) chiunque ha il diritto di esigere la rettifica o la cancellazione dei dati che lo riguardano contenenti errori di fatto o di diritto (art. 110).

d) chiunque ha il diritto di promuovere un'azione dinanzi alla giurisdizione o all'autorità competente in base alla legislazione nazionale, finalizzata ad assicurare il diritto di rettifica o di cancellazione (art. 111, 1° comma).

e) chiunque ha il diritto di verifica dei dati, esercitato presso l'autorità di controllo nazionale (art. 114, 2° comma).

L'ACC, tenendo conto in modo proporzionale ed equilibrato dei diritti della persona la cui identità è stata usurpata previsti dalla Convenzione di Schengen, nonché della necessità di individuare l'usurpatore, formula il seguente parere:

1. Alle segnalazioni nel SIS relative a persone la cui identità è stata usurpata si applica il diritto nazionale, fatte salve norme più rigorose previste dalla Convenzione (art. 104, 1° comma).

2. Spetta alla Parte contraente autrice della segnalazione garantire che i dati siano registrati per gli scopi enunciati e mantenerli attuali ed esatti (art. 102, 1° comma; art. 106, 1° comma, art. 110 e disposizioni in materia di protezione dei dati della Convenzione 108 del Consiglio d'Europa vincolanti per gli Stati Schengen, in particolare quelle dell'art. 5).

3. In conformità della procedura prevista dall'art. 106 della Convenzione, spetta alla Parte contraente autrice della segnalazione garantire l'esercizio del diritto di rettifica e di cancellazione dei dati registrati.

4. La conservazione nel SIS della segnalazione di una persona la cui identità è stata usurpata deve essere valutata secondo il principio della proporzionalità, tenuto conto, da un lato, dei diritti della persona la cui identità è stata usurpata e, dall'altro, della necessità di individuare l'usurpatore.

5. Nell'attesa che il SIS II sia messo in funzione, occorre studiare e adottare una soluzione adeguata e se possibile comune che consenta di indicare che si tratta di una segnalazione relativa ad un'identità usurpata. L'ACC esprime la sua volontà di collaborare per trovare tale soluzione.

6. *Parere 98/3 sulla trasmissione dei dati SIS relativi ai veicoli rubati alla banca dati Interpol «ASF¹⁰⁵⁾ - Veicoli rubati» (doc. SCH/Aut-cont (97) 50, 2^a rev.)*

Il progetto in questione, presentato in una nota del Comitato di orientamento SIS, mira a trasmettere ad una banca dati Interpol i dati del SIS relativi alle persone, ai veicoli rubati e, in un secondo tempo, ad altre categorie.

L'ACC ha richiamato diversi principi della Convenzione nonché il proprio parere sul progetto pilota Schengen sugli itinerari dei veicoli rubati e, limitandosi ai soli aspetti relativi alla protezione dei dati personali, ha formulato il seguente parere:

1. Le informazioni e i dati di natura personale inseriti nel Sistema d'informazione Schengen non possono essere trasmessi a Interpol nell'ambito del progetto «ASF - veicoli rubati» senza contravvenire alle disposizioni della Convenzione e in particolare agli artt. 101, 102, 118 e 126.

2. I dati relativi alla marca, al tipo, al colore e alle caratteristiche tecniche dei veicoli non sono dati di natura personale ai sensi della Convenzione.

3. La comunicazione di dati non personali ad Interpol nell'ambito del progetto «ASF - veicoli rubati» non viola le disposizioni della Convenzione in materia di protezione dei dati, a condizione che non sia possibile stabilire alcun collegamento con un dato che consenta di risalire all'identità di una persona in relazione con il veicolo.

4. Lo scambio di informazioni contenute negli archivi nazionali nel quadro della cooperazione di polizia è disciplinato dalla legislazione nazionale del paese interessato e, in particolare, dalla legge sulla protezione dei dati.

7. *Parere 98/4 del 3 febbraio 1998 sull'interpretazione dell'articolo 103 relativo al controllo dell'ammissibilità della consultazione del SIS (doc. SCH/Aut-cont (97) 70 riv.)*

L'attenzione dell'ACC è stata richiamata sulle difficoltà poste dall'applicazione dell'art. 103 della Convenzione, relativo alla registrazione ad opera dell'organo di gestione dell'archivio di ogni N.SIS di una trasmissione su dieci di dati personali, ai fini del controllo dell'ammissibilità dell'interrogazione

Consapevole del fatto che il Sistema d'Informazione Schengen (SIS) è un sistema di ricerca automatizzato che richiede un'efficace protezione contro l'accesso non autorizzato da parte di terzi, l'ACC ha considerato che la registrazione di una media rappresentativa delle consultazioni del sistema effettuate costituisce un mezzo di protezione adeguato contro tale accesso non autorizzato.

L'ACC ha avviato uno studio sulle soluzioni tecniche adottate in ogni Stato parte per rispettare il disposto dell'art. 103.

Ha constatato inoltre che le Parti contraenti interpretano in modo diverso l'obbligo imposto dalla Convenzione di registrare in media una trasmissione su dieci di dati di natura personale nella sezione nazionale del Sistema d'Informazione Schengen, ai fini del controllo dell'ammissibilità della consultazione (art. 103).

Ai fini di un'armonizzazione delle procedure applicate dalle Parti contraenti, l'ACC ha formulato un parere sull'interpretazione di questo articolo.

¹⁰⁵⁾ Automated Search Facility

Ritiene che la registrazione prevista all'art. 103 debba soddisfare i seguenti requisiti minimi:

1. Deve essere registrata una media sufficientemente rappresentativa di tutte le consultazioni, a prescindere dal fatto che alla relativa interrogazione venga data una risposta positiva o negativa. L'esigenza minima della registrazione del 10% può essere rispettata anche mediante una registrazione ad intervalli regolari.

2. Fanno parte degli elementi essenziali di un'adeguata registrazione:

a) le generalità trasmesse della persona oggetto della consultazione,
b) l'identificazione del terminale utilizzato o dell'autorità che ha proceduto all'interrogazione, badando a che siano adottate tutte le misure utili per consentire l'identificazione dell'utente,

c) il luogo, la data e l'ora della consultazione,

d) il motivo della consultazione, per es. indicazione del fondamento giuridico di una segnalazione.

3. Ai fini di un controllo, in singoli casi, dell'ammissibilità della consultazione sarebbe inoltre auspicabile indicare: il riferimento del dossier o il numero di protocollo della polizia per poter risalire al dossier di base, se disponibile.

I dati sono utilizzati esclusivamente ai fini previsti dall'art. 103.

I dati registrati vanno cancellati entro 6 mesi.

L'ACC insiste affinché si tenga conto dell'obbligo previsto dall'art. 103 in conformità del presente parere.

Capitolo V

PROGRAMMA D'AZIONE

Il programma d'azione proposto dal Presidente dell'ACC per il primo semestre del 1998 è stato approvato il 3 febbraio 1998.

Tale programma mira a rafforzare il ruolo dell'ACC nella struttura Schengen, definisce le priorità dei suoi interventi in difesa dei principi della protezione dei dati e raccomanda una maggiore cooperazione tra gli organi Schengen.

L'ACC proseguirà la propria missione di consulenza e di armonizzazione della prassi e delle dottrine nazionali formulando appositi pareri. Si assicurerà che Gruppo centrale riservi ai suoi pareri la necessaria pubblicità e, in caso contrario, determinerà in che modo garantirne la pubblicazione.

Particolare attenzione verrà dedicata all'attuazione, da parte degli organi esecutivi Schengen, delle raccomandazioni dell'ACC, in particolare in materia di sicurezza del C.SIS. Infatti, nonostante le due presidenze Schengen succedutesi nel 1997 abbiano affidato l'esame di tali raccomandazioni ai gruppi tecnici, è incontestabile che alla questione non sia stato riservato il carattere prioritario ritenuto necessario dall'ACC. Le prime risposte fornite il 4 marzo 1998 rivelano che le raccomandazioni dell'ACC non potranno essere implementate in tempi brevi. Questo vale, in particolare, per la richiesta dell'ACC di ricevere un «conto utente» per poter realizzare un audit sul sistema. Una tale soluzione consentirebbe di avere un accesso diretto, senza possibilità di modifica dei dati, al sistema operativo e alle basi dati e di procedere più facilmente al controllo del C.SIS.

L'ACC proseguirà i contatti con i rappresentanti del Ministero dell'Interno francese al fine di precisare le condizioni di realizzazione dei futuri controlli presso il C.SIS.

Provvederà alla diffusione presso i valichi autorizzati delle frontiere esterne Schengen dell'opuscolo sul diritto di accesso e di comunicazione al cittadino dei dati SIS che lo riguardano, il cui testo è stato approvato nel mese di dicembre 1997.

Intensificherà i contatti con i rappresentanti dell'Unione europea nella prospettiva dell'incorporazione dell'acquis Schengen nell'Unione europea partecipando, in particolare, alla definizione del proprio acquis.

In occasione della riunione che si terrà a Bruxelles il 27 e 28 aprile 1998, l'ACC presenterà la sua relazione annuale al pubblico e alla stampa.

Il 29 e il 30 giugno 1998 organizzerà a Lisbona un convegno sul tema «Diritti dei cittadini nei confronti dei sistemi di informazione di polizia - Il modello Schengen»

La realizzazione di questo programma d'azione si prefigge di contribuire all'affermazione del ruolo dell'ACC e dell'efficacia del suo intervento in difesa dei diritti e delle libertà dei cittadini in un contesto di consolidamento dello spazio europeo.

5.9.2 Parere n 98/1 - Conservazione dei dossier¹⁰⁶⁾

BPh/div.

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 55, 2^a rev.
Traduzione: orig.\DE

Parere n 98/1 dell'Autorità di controllo comune destinato al Comitato esecutivo

OGGETTO: Conservazione dei dossier ad avvenuta cancellazione di una segnalazione

In occasione della riunione del 3 febbraio 1998, l'Autorità di controllo comune (di seguito denominata ACC) ha adottato, sulla base dell'articolo 115, 3° comma della Convenzione di Schengen (di seguito denominata CSCH) il seguente parere:

Consapevole del fatto che servizi di polizia nazionali di determinate Parti contraenti continuano a conservare dossier anche ad avvenuta cancellazione di segnalazioni ex art. 95 e segg. CSCH e che ne fanno l'oggetto di fascicoli penali, che le autorità di polizia interessate si basano, in tale contesto, sulle disposizioni previste dal diritto nazionale in materia di protezione dei dati (cfr. punto 2.1.3, lettera *b*) del Manuale SIRENE e che si applicano anche le disposizioni di cui al Titolo VI della Convenzione di Schengen,

l'ACC ha esaminato questa prassi e al riguardo rinvia soprattutto alle seguenti esigenze attinenti al diritto in materia di protezione dei dati.

L'Autorità di controllo comune conferma i principi ed i diritti fondamentali in materia di protezione dei dati di cui alla Convenzione di Schengen, in particolare:

a) i dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (artt. 102, 1° comma e 94, 1° comma CSCH). Una deroga a tale principio generale è ammessa soltanto se giustificata dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la sicurezza pubblica dello Stato, per gravi ragioni di sicurezza dello Stato o ai fini della prevenzione di un fatto punibile grave (art. 107, 3° comma CSCH);

b) qualsiasi utilizzo dei dati non conforme ai commi da 1 a 4 dell'art. 102 sarà considerato uno sviamento di finalità (art. 102, 5° comma);

c) in conformità dell'articolo 112 CSCH, i dati personali inseriti nel Sistema d'Informazione Schengen ai fini della ricerca di persone sono conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti;

d) questi principi si applicano, nel quadro di un'interpretazione integrativa della Convenzione, a ogni tipo di trattamento dell'informazione relativo a segnalazioni contenute nel Sistema d'Informazione Schengen o basato sulle stesse.

¹⁰⁶⁾ Documento anticipato nella *Relazione per l'anno 1997*.

L'Autorità di controllo comune considera pertanto che si debbano adottare le seguenti misure:

a) in caso di soppressione di una segnalazione ai fini della ricerca di persone, ciascuna Parte contraente Schengen, in conformità dell'art. 112 CSCH, è tenuta a cancellare tale segnalazione e a distruggere senza indugio la corrispondente documentazione,

b) le autorità Schengen devono procedere ad una revisione del Manuale SIRENE allo scopo di cancellare le disposizioni contrarie di cui al suo punto 2.1.3 lettera b).

5.9.3 Parere n 98/2 - Segnalazione di persone la cui identità è stata usurpata¹⁰⁷⁾

BPh/div.

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 42, 2^a rev.
Traduzione: orig./PT

Parere n 98/2 dell'Autorità di controllo comune destinato al Comitato esecutivo

OGGETTO: Segnalazione nel Sistema d'Informazione Schengen di persone la cui identità è stata usurpata

L'ACC ha esaminato i problemi posti dall'utilizzazione abusiva di alias di persone segnalate nel SIS (vedasi le note SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 e SCH/Aut-cont (97) 42), alla luce dei principi di protezione dei dati di natura personale previsti dalla Convenzione di Schengen.

La segnalazione del titolare legittimo la cui identità è stata usurpata viene conservata nel SIS dalla maggioranza degli Stati. Attualmente non sembra possibile precisare nel SIS, quanto meno in testo libero, che si tratta di un caso d'identità usurpata.

L'ACC riafferma, in particolare, i seguenti principi e diritti fondamentali in materia di protezione dei dati:

a) i dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (articolo 102, primo comma e articolo 94, primo comma). Si tratta di un principio generale a cui si può derogare in via eccezionale se necessario per prevenire una minaccia grave o un reato grave (articolo 102, terzo comma).

b) qualunque utilizzazione dei dati non conforme ai commi da 1 a 4 dell'articolo 102 sarà considerata uno sviamento di finalità (articolo 102, quinto comma).

c) chiunque ha il diritto di esigere la rettifica o la cancellazione dei dati che lo riguardano contenenti errori di fatto o di diritto (articolo 110).

d) chiunque ha il diritto di promuovere un'azione dinanzi alla giurisdizione o all'autorità competente in base alla legislazione nazionale, finalizzata ad assicurare il diritto di rettifica o di cancellazione (articolo 111, primo comma).

e) chiunque ha il diritto di verifica dei dati, esercitato presso l'autorità di controllo nazionale (articolo 114, secondo comma).

L'ACC, tenendo conto in modo proporzionale ed equilibrato dei diritti della persona la cui identità è stata usurpata previsti dalla Convenzione di Schengen, nonché della necessità di individuare l'usurpatore, formula il seguente parere:

1. Alle segnalazioni nel SIS relative a persone la cui identità è stata usurpata si applica il diritto nazionale, fatte salve norme più rigorose previste dalla Convenzione (articolo 104, primo comma).

¹⁰⁷⁾ Documento anticipato nella *Relazione per l'anno 1997*.

2. Spetta alla Parte contraente autrice della segnalazione garantire che i dati siano registrati per gli scopi enunciati e mantenerli attuali ed esatti (articolo 102, primo comma, articolo 106, primo comma; articolo 110; disposizioni in materia di protezione dei dati della Convenzione 108 del Consiglio d'Europa vincolanti per gli Stati Schengen, in particolare quelle dell'articolo 5).

3. In conformità della procedura prevista dall'articolo 106 della Convenzione, spetta alla Parte contraente autrice della segnalazione garantire l'esercizio del diritto di rettifica e di cancellazione dei dati registrati.

4. La conservazione nel SIS della segnalazione di una persona la cui identità è stata usurpata deve essere valutata secondo il principio della proporzionalità, tenuto conto, da un lato, dei diritti della persona la cui identità è stata usurpata e, dall'altro, della necessità di individuare l'usurpatore.

5. Nell'attesa che il SIS sia messo in funzione, occorre studiare e adottare una soluzione adeguata e se possibile comune che consenta di indicare che si tratta di una segnalazione con identità usurpata. L'ACC esprime la sua volontà di collaborare per trovare tale soluzione.

5.9.4 Parere n 98/3 - Relazioni tra il Sistema d'informazione Schengen e il progetto «ASF - veicoli rubati»¹⁰⁸⁾

BPh/CP

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 3 dicembre 1997
SCH/Aut-cont (97) 50, 2^a rev.
Traduzione: orig. FR

Parere n 98/3 dell'Autorità di controllo comune all'attenzione del Comitato esecutivo

Relativo alle eventuali relazioni tra il Sistema d'informazione Schengen e il progetto ASF - veicoli rubati (Automated Search Facility) di Interpol (97) 81)

L'ACC è stata invitata ad esaminare una nota della delegazione tedesca del Comitato di orientamento SIS (doc. SCH/OR..SIS (97) 81) del 30 aprile 1997 nella quale si presenta il progetto «ASF - veicoli rubati (Automated Search Facility) in vista di una presa di posizione in ambito Schengen nei confronti di Interpol. Il progetto in questione spinge l'ACC a chiedersi se i dati SIS relativi alle persone e ai veicoli rubati possano essere trasmessi a Interpol.

La nota in oggetto descrive sommariamente il progetto: «Stando alle informazioni di cui dispone la delegazione tedesca, solo quattro Stati (Svezia, Lussemburgo, Russia e Slovacchia) partecipano attualmente alla parte del progetto relativa ai veicoli rubati. Sono disponibili attualmente record relativi a circa 80.000 veicoli rubati. (...) non solo per quanto riguarda in particolare le parti del progetto già in funzione relative alle persone e ai veicoli rubati, ma anche (...)».

È inoltre prevista l'estensione del progetto ad altre categorie di dati (opere d'arte, carte di credito, documenti e passaporti falsificati, navi/aerei rubati). Considerata l'importanza che possono assumere in futuro progetti di questo tipo, l'ACC ha deciso di formulare un parere in merito a questo progetto e di rispondere al quesito relativo alla possibilità di trasmettere a Interpol nell'ambito del progetto ASF i dati relativi alle persone e ai veicoli rubati.

Limitandosi ai soli aspetti relativi alla protezione dei dati di natura personale,

I'ACC

considerando che:

a) in virtù dell'articolo 101, quarto comma della Convenzione, solo le autorità sono autorizzate a consultare direttamente i dati inseriti nel SIS. A tal fine ciascuna Parte contraente comunica al Comitato esecutivo l'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel Sistema d'Informazione Schengen. L'elenco indica per ciascuna autorità i dati che essa può consultare e per quali missioni;

¹⁰⁸⁾ Documento anticipato nella *Relazione per l'anno 1997*.

b) in virtù dell'articolo 102, primo comma della Convenzione le Parti contraenti possono utilizzare i dati soltanto ai fini enunciati per ciascuna categoria di segnalazioni;

– in virtù dell'articolo 102, secondo comma della Convenzione, la duplicazione dei dati è vietata (salvo per motivi tecnici necessari per l'interrogazione diretta da parte della autorità competenti);

– in virtù dell'articolo 102, quarto comma della Convenzione, i dati non possono essere utilizzati per fini amministrativi;

– infine, in virtù dell'articolo 102, quinto comma della Convenzione, qualsiasi utilizzazione dei dati non conforme ai summenzionati commi di tale articolo sarà considerata uno sviamento di finalità;

c) in virtù dell'articolo 104, primo comma della Convenzione, fatte salve condizioni più rigorose previste dalla Convenzione, ai dati inseriti nella sezione nazionale del SIS si applica la legislazione nazionale;

d) in virtù dell'articolo 126, primo e secondo comma della Convenzione, le trasmissioni di dati di natura personale potranno avvenire solo verso le Parti contraenti che hanno adottato le disposizioni nazionali necessarie per ottenere un livello di protezione dei dati personali almeno pari a quello derivante dai principi della Convenzione del Consiglio d'Europa del 28 gennaio 1981;

e) in virtù dell'articolo 118, lettera d) della Convenzione, ogni Parte contraente si impegna ad impedire che persone non autorizzate utilizzino i sistemi di elaborazione automatizzata di dati mediante apparecchiature per la trasmissione di dati;

f) i dati relativi alla marca, al tipo, al colore e alle caratteristiche tecniche dei veicoli non sono dati di natura personale a condizione che non sia possibile stabilire un collegamento con un dato che consenta di identificare una persona in relazione con il veicolo come, ad esempio, il numero di targa o di telaio, e di risalire all'identità del proprietario o del conducente del veicolo;

g) le autorità di polizia di ogni paese partecipante al sistema ASF possono scambiare informazioni (nella fattispecie dati di natura personale) *provenienti da basi dati nazionali, nella misura in cui, mediante meccanismi di cooperazione di polizia bilaterale o multilaterale*, questo scambio di informazioni sia autorizzato o non sia vietato dalla legislazione nazionale in materia di protezione dei dati;

h) si deve tener conto del parere dell'ACC del 7 marzo 1997 relativo al progetto pilota sui veicoli rubati (v. doc. SCH/Aut-cont (97) 22 riv.). In tale parere si trattava di determinare se i paesi non ancora integrati nel Sistema di informazione Schengen possono avere accesso ai dati del SIS riguardanti i veicoli rubati;

FORMULA IL SEGUENTE PARERE:

1. Le informazioni e i dati di natura personale inseriti nel Sistema d'informazione Schengen non possono essere trasmessi a Interpol nell'ambito del progetto «ASF - veicoli rubati» senza contravvenire alle disposizioni della Convenzione e in particolare agli articoli 101, 102, 118 e 126.

2. I dati relativi alla marca, al tipo, al colore e alle caratteristiche tecniche dei veicoli non sono dati di natura personale ai sensi della Convenzione.

3. La comunicazione di dati non personali ad Interpol nell'ambito del progetto «ASF - veicoli rubati» non viola le disposizioni della Convenzione in materia di protezione dei dati, a condizione che non sia possibile stabilire alcun collegamento con un dato che consenta di risalire all'identità di una persona in relazione con il veicolo.

4. Lo scambio di informazioni nel quadro della cooperazione di polizia, basato sulle informazioni contenute negli archivi nazionali, è disciplinato dalla legislazione del paese interessato e, in particolare, dalla legge sulla protezione dei dati.

5.9.5 Parere n 98/4 - Registrazione delle consultazioni di cui all'art. 103 della Convenzione¹⁰⁹⁾

BPh/div.

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 70 riv.
Traduzione: orig.\DE

Parere n. 98/4 dell'Autorità di controllo comune destinato al Comitato esecutivo

OGGETTO: Registrazione delle consultazioni di cui all'articolo 103 della Convenzione

L'Autorità di controllo comune,

Visto l'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen;

Consapevole del fatto che il Sistema d'Informazione Schengen (SIS) è un sistema di ricerca automatizzato che richiede un'efficace protezione contro l'accesso non autorizzato da parte di terzi,

che la registrazione di una media rappresentativa delle consultazioni del sistema effettuate costituisce un mezzo di protezione adeguato contro l'accesso non autorizzato,

che l'articolo 103 CSCH impone a ciascuna Parte contraente di provvedere affinché una trasmissione in media su dieci di dati personali sia registrata nella sezione nazionale del Sistema d'Informazione Schengen dall'organo di gestione dell'archivio, ai fini del controllo dell'ammissibilità dell'interrogazione, ritiene necessarie le seguenti esigenze minime per quanto concerne una regolare registrazione ai sensi dell'art. 103 CSCH:

1. Deve essere registrata una media sufficientemente rappresentativa di tutte le consultazioni, a prescindere dal fatto che alla relativa interrogazione venga data una risposta positiva o negativa. L'esigenza minima della registrazione del 10% può essere rispettata anche mediante una registrazione ad intervalli regolari.

2. Fanno parte degli elementi essenziali di un'adeguata registrazione:

- a) generalità trasmesse della persona oggetto della consultazione,
- b) identificazione del terminale utilizzato o dell'autorità che ha proceduto all'interrogazione, badando a che siano adottate tutte le misure utili per consentire l'identificazione dell'utente,
- c) luogo, data e ora della consultazione,
- d) motivo della consultazione, per es. indicazione del fondamento giuridico di una segnalazione.

¹⁰⁹⁾ Documento anticipato nella *Relazione per l'anno 1997*.

3. Ai fini di un controllo, in singoli casi, dell'ammissibilità della consultazione sarebbe inoltre auspicabile indicare il riferimento del dossier o il numero di base, se disponibile.

4. I dati sono utilizzati esclusivamente ai fini previsti dall'art. 103.

5. I dati registrati vanno cancellati entro 6 mesi.

L'ACC insiste affinché si tenga conto dell'obbligo previsto dall'art. 103 in conformità del presente parere.

5.9.6 Relazione sulla sicurezza degli uffici SIRENE

/div.

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 11 dicembre 1998
SCH/Aut-cont (98) 47, 2^a rev.
Traduzione: orig./FR-PT

Progetto**Relazione dell'ACC sulla sicurezza degli uffici SIRENE**

In occasione della riunione del 12 dicembre 1997, l'Autorità di controllo comune ha deciso di procedere alla verifica delle misure di sicurezza messe in atto dagli Uffici SIRENE. Tale decisione è stata adottata in seguito alla fuga di documenti avvenuta tempo addietro in un Ufficio SIRENE.

Tutti i membri dell'ACC dei paesi che applicano la Convenzione hanno quindi effettuato controlli nei rispettivi uffici SIRENE e hanno trasmesso la loro relazione al Segretariato dell'ACC, i cui membri hanno annunciato che avrebbero presentato una relazione complementare.

Le relazioni delle autorità nazionali descrivono la situazione nei settori della sicurezza fisica e delle comunicazioni tra l'ufficio SIRENE e l'N.SIS; descrivono inoltre le funzioni di tracciatura, che consentono, non solo di rintracciare l'ufficio e il terminale, ma anche di identificare l'operatore che ha utilizzato un applicativo (ad esempio per un aggiornamento), nonché le condizioni di accesso ai dati del SIS e agli archivi manuali ¹¹⁰⁾.

Alla luce delle precedenti constatazioni, l'ACC conclude che sono stati prodigati sforzi al fine di migliorare la sicurezza del sistema ma che questi devono proseguire.

L'ACC richiama infatti i seguenti principi:

- gli uffici SIRENE devono soddisfare tutte le condizioni contemplate all'articolo 118 della Convenzione di applicazione di Schengen;
- il livello di sicurezza degli uffici SIRENE nazionali non può essere inferiore a quello del SIS.

Premesso ciò, l'ACC propone che negli Stati dove tali principi non sono ancora applicati vadano prese le seguenti disposizioni:

1. mantenimento della sicurezza fisica al massimo livello aggiornando le tecniche impiegate. Negli Stati in cui sono state constatate lacune, vanno apportate le modifiche necessarie quanto prima e va informata l'autorità di controllo nazionale;

¹¹⁰⁾ Trattasi delle relazioni SCH/Aut-cont (98) 9 della Francia, 13 e 40 del Belgio, 15 dell'Italia, 21 della Germania, 28 della Grecia, 31 del Portogallo, 33 dei Paesi Bassi, 35 della Spagna e 36 dell'Austria. La relazione sulla sicurezza dell'ufficio SIRENE lussemburghese figura nella relazione annuale dell'autorità di controllo lussemburghese e sarà completata prossimamente da una nuova relazione. Anche i Paesi Bassi comunicheranno fra breve una nuova relazione di controllo.

2. cifratura delle comunicazioni tra il SIRENE e l'N.SIS e controllo della cifratura da parte dei membri delle autorità;

3. a) realizzazione di un sistema di tracciatura di tutte le operazioni possibili riguardanti la base di dati N.SIS e dell'ufficio SIRENE (numero di interrogazioni, orario, tipi di dati consultati, ecc.);

b) analisi regolare degli archivi di tracciatura al fine di individuare eventuali anomalie riguardo, in particolare, al numero di interrogazioni;

4. limitazione e controllo dell'accesso agli archivi manuali dei dossier;

5. cifratura delle informazioni contenute su supporto informatico;

6. a) intensificazione delle misure di sicurezza al fine di garantire che l'accesso sia effettivamente limitato ai dati per i quali gli operatori hanno un'autorizzazione, in particolare verificando regolarmente le loro autorizzazioni di accesso e modificando regolarmente le password;

b) verifica regolare dei motivi di una interrogazione del SIS;

7. designazione di un funzionario responsabile della sicurezza e definizione delle norme di sicurezza comuni ai vari uffici SIRENE, applicabili al loro personale;

8. organizzazione della gestione delle informazioni stampate in modo da limitare l'ottenimento di stampe dello schermo contenenti informazioni della base di dati SIRENE e di segnalazioni SIS;

9. *inserimento* dell'organizzazione di corsi di formazione incentrati sulla sicurezza dei dati per gli utenti degli uffici SIRENE;

10. raccomandazione dell'elaborazione da parte degli N.SIS e degli uffici SIRENE di relazioni sulla sicurezza, a intervalli regolari, per esempio ogni anno.

L'evoluzione futura del sistema di comunicazione dei dati tra gli Stati, per quanto riguarda in particolare lo sviluppo del SIS, dovrà obbligatoriamente tenere conto delle condizioni di sicurezza, qualunque sia il modello, centralizzato o non centralizzato, prescelto.

Infine, l'ACC sottolinea la cooperazione di tutte le autorità nazionali interessate ed esprime la sua soddisfazione per il fatto che questa operazione di verifica condotta in modo coordinato in tutti gli Stati ha contribuito a migliorare sensibilmente la sicurezza delle informazioni. Ciò è fondamentale per la fiducia dei cittadini e delle istituzioni democratiche nel funzionamento del Sistema Schengen.

5.9.7 Dichiarazione in occasione del 50° Anniversario della dichiarazione universale dei diritti dell'uomo

BPH/BG

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 11 dicembre 1998

SCH/Aut-cont (98) 66

Traduzione: orig./FR

b;Dichiarazione dell'Autorità di controllo comune di Schengen in occasione del 50° anniversario della Dichiarazione universale dei diritti dell'uomo

«In occasione del 50° anniversario della Dichiarazione universale dei diritti dell'Uomo, commemorata il 10 dicembre 1998, l'Autorità di controllo comune di Schengen riunitasi a Bruxelles l'11 dicembre esprime il suo impegno nella difesa dei diritti dei cittadini rispetto al sistema d'informazione Schengen, affermando così concretamente i grandi valori della libertà e dei diritti dell'Uomo sanciti dalla Dichiarazione universale».

5.10 CONSIGLIO D'EUROPA

5.10.1 Raccomandazione n. 99 (5) - Linee guida per la protezione della privacy su Internet

Raccomandazione N. R (99) 5 del Comitato dei Ministri agli Stati membri per la protezione della privacy su internet

LINEE-GUIDA

per la protezione delle persone rispetto alla raccolta
e al trattamento di dati personali sulle autostrade dell'informazione
(adottate dal Comitato dei Ministri il 23 febbraio 1999
nel corso della 660ma riunione dei Delegati dei Ministri)

PREAMBOLO

Il Comitato dei Ministri, ai sensi dell'articolo 15.b dello Statuto del Consiglio d'Europa,

Considerando che scopo del Consiglio d'Europa è quello di realizzare un'unione più stretta fra i suoi membri;

Rilevando lo sviluppo delle nuove tecnologie e dei nuovi servizi di comunicazione e di informazione on-line;

Consapevole che tale sviluppo influirà notevolmente sul funzionamento della società in genere e sui rapporti fra le persone, in particolare offrendo possibilità ulteriori di comunicazione e di scambio di informazioni sul piano nazionale e internazionale;

Consapevole dei vantaggi che gli utilizzatori delle nuove tecnologie possono ricavare da tale sviluppo;

Ritenendo, comunque, che lo sviluppo delle tecnologie e la generalizzazione della raccolta e del trattamento di dati personali sulle autostrade dell'informazione comportino rischi per la *privacy* delle persone fisiche;

Ritenendo che gli sviluppi tecnologici permettano anche di contribuire al rispetto dei diritti e delle libertà fondamentali, e in particolare del diritto alla *privacy*, all'atto del trattamento di dati personali relativi a persone fisiche;

Consapevole della necessità di mettere a punto tecniche che consentano l'anonimato degli interessati e la segretezza delle informazioni scambiate attraverso le autostrade dell'informazione, nel rispetto dei diritti e delle libertà altrui e dei valori di una società democratica;

Consapevole che le comunicazioni effettuate con l'ausilio delle nuove tecnologie dell'informazione sono egualmente soggette al rispetto dei diritti dell'uomo e delle libertà fondamentali, e in particolare del diritto al rispetto della *privacy* e della segretezza della corrispondenza, così come sanciti dall'articolo 8 della Convenzione europea dei diritti dell'uomo;

Riconoscendo che la raccolta, il trattamento e in particolare la comunicazione di dati personali attraverso le nuove tecnologie dell'informazione, e in particolare attraverso le autostrade dell'informazione, sono regolati dalle disposizioni della Convenzione per la protezione delle persone rispetto al trattamento automatico di dati personali (Strasburgo 1981, ETS N. 108) e da raccomandazioni

settoriali in materia di protezione dei dati, e in particolare dalla Raccomandazione N. R (90) 19 sulla protezione dei dati personali utilizzati per finalità di pagamento e altre finalità correlate, dalla Raccomandazione N. R (91) 10 sulla comunicazione a terzi di dati personali detenuti da soggetti pubblici e dalla Raccomandazione N. R (95) 4 sulla protezione dei dati personali nel settore delle telecomunicazioni, con particolare riferimento ai servizi telefonici;

Ritenendo che sia opportuno sensibilizzare utilizzatori e fornitori di servizi Internet in merito alle disposizioni generali della Convenzione prima ricordata relativamente alla raccolta e al trattamento di dati personali sulle autostrade dell'informazione;

Raccomanda ai governi degli Stati membri di dare ampia diffusione alle Linee-guida contenute nell'allegato alla presente Raccomandazione, in particolare presso gli utilizzatori e i fornitori di servizi su Internet, nonché presso tutte le autorità nazionali incaricate di verificare il rispetto delle disposizioni in materia di protezione dei dati.

ALLEGATO

alla Raccomandazione N. R (99) 5 del
Comitato dei Ministri agli Stati membri
per la protezione della *privacy* su Internet

LINEE-GUIDA PER LA PROTEZIONE DELLE PERSONE RISPETTO ALLA RACCOLTA E AL TRATTAMENTO DI DATI PERSONALI SULLE AUTOSTRADE DELL'INFORMAZIONE EVENTUALMENTE DA INSERIRE IN O ALLEGARE A CODICI DEONTOLOGICI

I. INTRODUZIONE

Le presenti linee-guida enunciano i principi di una prassi corretta in materia di *privacy* per gli utenti e i fornitori di servizi Internet (FSI) ¹¹¹⁾. Questi principi possono essere ripresi nell'ambito di codici deontologici.

Gli utenti dovrebbero essere a conoscenza delle responsabilità dei fornitori di servizi Internet (FSI), e viceversa. Pertanto, è opportuno che utenti e fornitori di servizi leggano il testo nella sua interezza, anche se per facilitarne l'impiego esso si presenta suddiviso in più parti. Possono risultare pertinenti le linee-guida di una sola parte ovvero di più parti.

L'uso di Internet comporta responsabilità per ciascuna delle vostre azioni ed implica inoltre rischi per la *privacy*. È importante adottare comportamenti che offrano protezione a voi e favoriscano rapporti positivi con gli altri. In questo documento vengono offerti alcuni suggerimenti pratici per tutelare la *privacy*, ma dovrete conoscere anche i diritti e gli obblighi cui siete legalmente soggetti.

Ricordate che il rispetto per la *privacy* è un diritto fondamentale delle persone che può essere tutelato per legge, e in particolare attraverso norme per la protezione dei dati, per cui può essere senz'altro il caso di verificare la vostra situazione giuridica.

¹¹¹⁾ V. Parte IV, primo paragrafo.

II. PER GLI UTENTI

1. Ricordate che Internet non è sicuro. Tuttavia, esistono e vengono continuamente messi a punto strumenti che permettono di migliorare la protezione dei vostri dati ¹¹²⁾. Utilizzate dunque tutti gli strumenti disponibili per proteggere i vostri dati e le vostre comunicazioni, ad esempio le forme legalmente ammesse di cifratura per garantire la segretezza della posta elettronica e codici di accesso per il vostro personal computer ¹¹³⁾.

2. Ricordate che ogni transazione compiuta, ogni sito visitato su Internet lascia una traccia. Queste «tracce elettroniche» possono essere utilizzate, a vostra insaputa, per generare un profilo delle vostre caratteristiche e dei vostri interessi. Se non desiderate la creazione di tali profili, siete invitati a utilizzare gli strumenti tecnici più recenti che prevedono la possibilità di venire informati ogniqualevolta si lascia una traccia, e di rifiutare queste tracce. Potete inoltre informarvi sulle politiche in materia di *privacy* dei singoli siti e programmi, preferendo quelli che registrano pochi dati o che sono accessibili in forma anonima.

3. La migliore forma di tutela della *privacy* è rappresentata dall'anonimato nell'accesso e nell'utilizzazione di servizi, e dalla disponibilità di forme anonime di pagamento. Informatevi sulle possibilità tecniche per ottenere l'anonimato, laddove ciò sia opportuno ¹¹⁴⁾.

4. L'anonimato assoluto può non essere appropriato a causa di limitazioni di ordine giuridico. In tal caso, se la legge lo consente, potete utilizzare uno pseudonimo in modo che la vostra identità personale sia nota solo al vostro FSI.

5. Comunicate al vostro FSI, e ad ogni altro soggetto, solo i dati che sono necessari per una specifica finalità di cui siete stati messi al corrente. Fate particolare attenzione alle carte di credito e ai numeri di conto, che su Internet possono essere utilizzati anche in modi impropri con grande facilità.

6. Ricordate che il vostro indirizzo di posta elettronica costituisce un dato personale, e che altri potrebbero desiderare di utilizzarlo per scopi diversi, ad esempio per l'inserimento in annuari o elenchi di utenti. Non esitate a informarvi sulle finalità dell'annuario o di ogni altra utilizzazione. Potete chiedere che il vostro indirizzo sia cancellato se non desiderate figurare in un elenco.

7. Siate prudenti con i siti che chiedono dati aggiuntivi rispetto a quelli necessari per accedere al sito o compiere una determinata operazione, oppure che non vi dicono per quale motivo abbiano necessità di ottenere da voi questi dati.

8. Ricordate che siete legalmente responsabili per il trattamento dei dati, ad esempio in caso di caricamento o scaricamento illeciti, e che potete essere sempre rintracciati anche se vi servite di uno pseudonimo.

9. Non inviate messaggi di disturbo. Possono ritorcersi contro di voi e avere conseguenze legali.

10. Il vostro FSI ha la responsabilità di compiere un utilizzo corretto dei dati. Chiedete al vostro FSI quali dati raccoglie, tratta e registra, in che modo e per quali finalità. Ripetete questa richiesta a intervalli regolari. Insistete affinché il

¹¹²⁾ Il termine «dati» è riferito ai «dati personali» e indica qualsiasi informazione riguardante voi o altre persone.

¹¹³⁾ Ad esempio, utilizzate una parola-chiave e modificatela regolarmente.

¹¹⁴⁾ Ad esempio, utilizzando posti pubblici Internet oppure carte d'accesso prepagate e carte di pagamento.

vostro FSI modifichi i dati se non sono corretti, o li cancelli se sono eccessivi, non aggiornati o non più necessari. Chiedete al FSI di informare di queste modifiche le altre parti alle quali abbia comunicato i vostri dati ¹¹⁵⁾.

11. Se non siete soddisfatti del modo in cui il vostro attuale FSI raccoglie, utilizza, registra o comunica dati, e se il FSI rifiuta di modificare i propri comportamenti, prendete in considerazione la possibilità di rivolgervi a un altro FSI. Se ritenete che il vostro FSI non rispetti le norme in materia di protezione dati, potete informare le autorità competenti oppure adire le vie legali.

12. Tenetevi al corrente dei rischi per la *privacy* e la sicurezza su Internet e degli strumenti disponibili per ridurre tali rischi.

13. Se avete intenzione di inviare dati in un altro Paese, dovrete essere consapevoli del fatto che là essi possono godere di una protezione minore. Se si tratta di dati che vi riguardano, siete evidentemente liberi di trasmetterli in ogni caso. Tuttavia, prima di inviare in un altro Paese dati relativi ad altre persone, dovrete informarvi sulla possibilità di effettuare il trasferimento in questione ¹¹⁶⁾ - ad esempio, presso le autorità competenti nel vostro Paese. Potrebbe essere necessario chiedere al destinatario di adottare le misure ¹¹⁷⁾ necessarie a garantire la protezione dei dati.

III. PER I FORNITORI DI SERVIZI SU INTERNET

1. Utilizzate le procedure corrette e le tecnologie disponibili, preferibilmente quelle che sono oggetto di una certificazione, per tutelare la *privacy* degli interessati (anche se non utilizzano Internet), in particolare garantendo l'integrità e la segretezza dei dati nonché la sicurezza fisica e logica della rete e dei servizi forniti sulla rete.

2. Informate gli utenti dei rischi per la *privacy* associati all'utilizzo di Internet prima che essi si mettano in lista per un servizio o lo utilizzino. Può trattarsi di rischi per l'integrità dei dati, la segretezza, la sicurezza della rete oppure di altri rischi per la *privacy* quali la raccolta o la registrazione occulte di dati.

3. Informate gli utenti degli strumenti tecnici che possono legittimamente utilizzare per ridurre i rischi a carico della sicurezza dei dati e delle comunicazioni, quali le forme di cifratura e di firma digitale ammesse dalla legge. Offrite questi strumenti tecnici a un prezzo definito dai costi effettivi e non dissuasivo.

4. Prima di accettare abbonamenti e di collegare utenti a Internet, informateli delle possibilità di accedere in modo anonimo a Internet, e di utilizzarne e pagarne i servizi mantenendo l'anonimato (ad esempio, attraverso carte di accesso prepagate). Talora l'anonimato totale non è indicato a causa di limitazioni di legge. In casi del genere, se la legge lo consente, offrite la possibilità di utiliz-

¹¹⁵⁾ La legislazione in materia di protezione dei dati, conformemente all'art. 5 della Convenzione per la protezione dei dati elaborata dal Consiglio d'Europa, prevede che il soggetto che tratta i dati sia responsabile dell'esattezza e dell'aggiornamento dei dati stessi.

¹¹⁶⁾ La legislazione di numerosi Paesi europei proibisce il trasferimento verso Paesi che non garantiscano un livello di protezione dei dati adeguato o equivalente a quello del vostro Paese. Sono comunque previste alcune eccezioni, in particolare se l'interessato ha acconsentito al trasferimento dei propri dati verso un Paese del tipo suddetto.

¹¹⁷⁾ Può trattarsi di garanzie sviluppate e/o presentate, in particolare nell'ambito del contratto che regola il flusso transfrontaliero dei dati.

zare pseudonimi. Informate gli utenti sui programmi che permettono di effettuare ricerche e navigare sul Web in modo anonimo. Configurate il vostro sistema in modo da evitare o ridurre al minimo l'utilizzazione di dati personali.

5. Non leggete, modificate o cancellate messaggi inviati ad altri.

6. Non permettete alcuna ingerenza nel contenuto di comunicazioni, a meno che tale ingerenza sia prevista dalla legge ed attuata da una pubblica autorità.

7. Raccogliete, trattate e registrate dati personali relativi agli utenti solo se ciò è necessario per scopi espliciti, specifici e legittimi.

8. Non comunicate dati a terzi se non nei casi previsti dalla legge ¹¹⁸⁾.

9. Non conservate i dati per un periodo superiore a quello necessario per realizzare le finalità del trattamento ¹¹⁹⁾.

10. Utilizzate dati personali per i vostri scopi promozionali o di marketing solo se l'interessato, una volta informato, non vi si è opposto oppure, nel caso del trattamento di dati relativi al traffico o di dati sensibili, ha dato il proprio consenso esplicito.

11. Siete responsabili dell'utilizzo corretto dei dati. Indicate in modo chiaro e visibile la vostra politica in materia di *privacy* sulla pagina iniziale del sito. Tale indicazione dovrebbe consentire di accedere, attraverso un legame ipertestuale, a una spiegazione dettagliata della prassi adottata in materia di *privacy*. Prima che l'utente inizi a utilizzare i servizi disponibili, all'atto di visitare il vostro sito e ogniqualvolta ne faccia richiesta, informatelo sulla vostra identità, sui dati che raccogliete, trattate e conservate, sulle modalità relative, le finalità e il periodo di conservazione. Se occorre, chiedete il suo consenso. Su richiesta dell'interessato, correggete senza indugio i dati inesatti, cancellateli se sono eccessivi, non più aggiornati o non più necessari, e bloccate il trattamento dei dati se l'utente vi si oppone. Informate di qualsiasi modifica i terzi ai quali avete comunicato i dati. Evitate di raccogliere dati in modi occulti.

12. Le informazioni fornite agli utenti devono essere accurate e aggiornate.

13. Pensateci due volte prima di pubblicare dati sul vostro sito! Così facendo potreste violare la *privacy* altrui e forse commettereste un reato.

14. Prima di inviare dati in un altro Paese, informatevi sull'ammissibilità del trasferimento - ad esempio presso le autorità competenti nel vostro Paese. Potrebbe essere necessario chiedere al destinatario di fornire garanzie indispensabili a garantire la protezione dei dati.

IV. CHIARIMENTI E MEZZI DI TUTELA

1. Quando nel presente testo si utilizza il termine «fornitore di servizio», esso si intende riferito, se del caso, anche agli altri operatori su Internet - fornitori di accesso, di contenuti, gestori di rete, ideatori dei programmi di navigazione, moderatori di gruppi di discussione, ecc.

¹¹⁸⁾ In genere la legislazione in materia di dati personali consente la comunicazione a terzi nel rispetto di specifiche condizioni, e in particolare

– per quanto riguarda dati sensibili e dati sul traffico, purché l'interessato abbia dato esplicitamente il proprio consenso;

– per quanto riguarda gli altri dati, se la comunicazione è necessaria per raggiungere la finalità legittima perseguita, ovvero se l'interessato, dopo esserne stato informato, non vi si è opposto.

¹¹⁹⁾ Ad esempio, non conservate dati relativi alla fatturazione se ciò non è previsto dalla legge.

2. È importante che vi assicuriate del rispetto dei vostri diritti. I meccanismi di *feed-back* offerti da gruppi di utenti di Internet, associazioni di fornitori di servizi Internet, autorità di protezione dati o altri soggetti sono strumenti importanti per garantire il rispetto delle presenti linee-guida. Contattate questi soggetti se avete bisogno di chiarimenti o di mezzi di tutela.

3. Le presenti linee-guida si applicano a tutte le autostrade informatiche.

5.10.2 Schema di raccomandazione - Protezione dei dati personali raccolti e trattati per scopi assicurativi

Schema di raccomandazione sulla protezione dei dati personali raccolti e trattati per scopi assicurativi

In previsione della 18^{ma} riunione del Bureau del CJ-PD - 19/21 gennaio 1999

PREAMBOLO

Il Comitato dei Ministri, ai sensi dell'articolo 15.b dello Statuto del Consiglio d'Europa:

1. Considerando che lo scopo del Consiglio di Europa è quello di realizzare una unione più stretta fra i suoi membri;

2. Richiamandosi ai principi generali relativi alla protezione dei dati contenuti nella Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati personali, e in particolare all'articolo 6 di tale Convenzione, in cui si afferma che i dati personali classificati come sensibili non possono essere sottoposti a trattamento se il diritto interno non prevede garanzie appropriate;

3. Consapevole del fatto che il trattamento automatizzato di dati personali per scopi assicurativi trova crescente diffusione, non solo per la preparazione, la stipula, l'esecuzione e la risoluzione di contratti assicurativi, ma anche per facilitare la gestione razionale ed economica delle assicurazioni e per la lotta alle frodi;

4. Consapevole del fatto che le assicurazioni sono fornite da vari soggetti economici, in particolare da compagnie assicurative;

5. Convinto dell'importanza che la qualità, l'integrità e la disponibilità dei dati personali rivestono per gli assicurati;

6. Rilevando che in pratica l'intera popolazione degli Stati membri è interessata da uno o più contratti assicurativi, e che per tale motivo i professionisti nel campo delle assicurazioni sono in possesso di una grande quantità di dati personali, alcuni dei quali sensibili;

7. Convinto dell'opportunità di regolamentare la raccolta e il trattamento di dati personali per scopi assicurativi, di garantire segretezza e sicurezza di tali dati personali e di verificare che ne venga compiuto un uso rispettoso dei diritti e delle libertà fondamentali dell'individuo, e in particolare del diritto alla riservatezza;

8. Tenendo conto del fatto che la mobilità dei singoli e la globalizzazione dei mercati e delle attività commerciali impongono lo scambio transfrontaliero di informazioni anche nel settore assicurativo, e richiedono una protezione dei dati equivalente in tutti gli Stati membri del Consiglio d'Europa,

RACCOMANDA AI GOVERNI DEGLI STATI MEMBRI:

1. di prendere provvedimenti affinché i principi contenuti nell'allegato alla presente Raccomandazione siano rispecchiati dal diritto interno e dalle prassi rispettive;

2. di assicurare un'ampia diffusione dei principi contenuti nell'allegato alla presente Raccomandazione presso tutte le persone, le pubbliche autorità e tutti gli enti pubblici o privati che raccolgono e trattano dati personali per scopi assicurativi, nonché presso gli enti competenti in materia di protezione dei dati;

3. di promuovere l'accettazione e l'attuazione dei principi contenuti nell'allegato alla presente Raccomandazione, in particolare attraverso l'adozione di disposizioni di legge o favorendo la definizione di un codice deontologico.

Decide che la Raccomandazione N. 86(1), sulla protezione di dati personali utilizzati per scopi di previdenza sociale, si applica alla raccolta ed al trattamento di dati per scopi di previdenza sociale nella misura in cui essi non siano regolamentati dalla presente Raccomandazione.

ALLEGATO

1. DEFINIZIONI

Ai fini della presente Raccomandazione:

a) per «dati personali» si intendono tutte le informazioni riguardanti una persona fisica identificata o identificabile («interessato»). Una persona fisica non si considera identificabile se tale identificazione richiede tempi e attività non ragionevoli.

b) per «dati sensibili» si intendono dati personali che rivelino l'origine razziale, le opinioni politiche, le fedi religiose o di altra natura, nonché i dati personali relativi alla salute, alla vita sessuale o alle condanne penali, e ogni altro dato definito sensibile ai sensi del diritto interno.

c) per «dati genetici» si intendono tutti i dati, indipendentemente dalla tipologia, che riguardano i caratteri ereditari di un individuo o le modalità di trasmissione di tali caratteri nell'ambito di un gruppo di individui legati da vincoli di parentela.

d) per «dati assicurativi» si intendono tutti i dati personali raccolti e trattati a scopi assicurativi.

e) l'espressione «per scopi assicurativi» comprende tutte le operazioni che comportano la raccolta e il trattamento di dati personali relativi alla preparazione, all'esecuzione e alla risoluzione di un contratto assicurativo.

f) per «trattamento» si intende ogni operazione o insieme di operazioni effettuate in tutto o in parte con l'ausilio di procedure automatizzate e applicate a dati personali, quali la registrazione, la conservazione o alterazione, l'estrazione, la consultazione, l'utilizzazione, la comunicazione, la comparazione o interconnessione e la cancellazione o la distruzione.

g) per «comunicazione» si intende l'atto di rendere dati personali accessibili a terzi, indipendentemente dagli strumenti o dai supporti utilizzati.

h) per «titolare dei dati assicurativi» si intende la persona fisica o giuridica, la pubblica autorità, l'organismo od ogni altro ente che, da solo o congiuntamente con altri, definisce le finalità e i metodi della raccolta e del trattamento di dati assicurativi.

2. CAMPO DI APPLICAZIONE

2.1 La presente Raccomandazione si applica alla raccolta e al trattamento di dati assicurativi.

2.2 Gli Stati membri sono invitati ad estendere l'applicazione della presente Raccomandazione al trattamento non automatizzato di dati personali per scopi assicurativi.

2.3 Non si devono sottoporre dati personali a trattamenti non automatizzati per evitare l'applicazione dei principi stabiliti nella presente Raccomandazione.

2.4 Gli Stati membri possono estendere i principi sanciti nella presente Raccomandazione alla raccolta e al trattamento di dati relativi a gruppi di persone, associazioni, fondazioni, società, società per azioni e ogni altro ente costituito direttamente o indirettamente da persone fisiche, indipendentemente dal fatto che tali enti siano dotati di personalità giuridica.

2.5 Gli Stati membri possono estendere i principi sanciti nella presente Raccomandazione alla protezione dei dati personali utilizzati per scopi di previdenza sociale.

3. RISPETTO PER LA VITA PRIVATA

3.1. Durante la raccolta ed il trattamento di dati personali occorre garantire il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata.

3.2. Le persone che, nel corso di un'attività assicurativa, hanno accesso a dati personali devono, conformemente al diritto e alla prassi interni, sottostare a norme di segretezza. In particolare, la raccolta ed il trattamento di dati sanitari devono essere effettuati unicamente da professionisti in campo sanitario, ovvero in conformità a norme di segretezza paragonabili a quelle applicabili ai professionisti in campo sanitario o in conformità a garanzie di pari efficacia previste dal diritto interno.

4. RACCOLTA E TRATTAMENTO DI DATI ASSICURATIVI

4.1 La raccolta e il trattamento (compresa la comunicazione) di dati assicurativi sono effettuati in modo corretto e legittimo ed esclusivamente per specifici scopi assicurativi, tranne nei casi previsti ai principi 4.10 e 8.1. I dati assicurativi devono essere adeguati, esatti, pertinenti e non eccessivi in rapporto agli scopi per i quali sono raccolti o successivamente trattati.

4.2. In linea di principio, i dati assicurativi sono raccolti presso l'interessato o il suo rappresentante legale.

Legittimità

4.3 La raccolta ed il trattamento di dati assicurativi sono consentiti:

a) se ciò è previsto da norme di legge, in particolare ai fini dell'assicurazione obbligatoria;

b) per la conclusione, l'esecuzione e la risoluzione di un contratto assicurativo stipulato con l'interessato, e per la preparazione di tale contratto su richiesta dell'interessato;

c) se l'interessato o il suo rappresentante legale o un'autorità od ogni altra persona o ente indicati per legge hanno dato il consenso per uno o più scopi assicurativi, e nella misura in cui ciò non contrasti con le norme di diritto interno; ovvero

d) se i dati sono necessari per il perseguimento degli interessi legittimi del titolare dei dati assicurativi, nella misura in cui non prevalgano gli interessi dell'interessato.

Scopi

4.4. Salvo quanto disposto ai punti da 4.6 a 4.11, la raccolta ed il trattamento di dati assicurativi sono consentiti esclusivamente per i seguenti scopi:

- a) preparazione ed emissione di un contratto assicurativo;
- b) raccolta di premi e altre forme di fatturazione;
- c) regolamento crediti o pagamento di altri benefici/indennità;
- d) riassicurazioni;
- e) assicurazioni congiunte;
- f) prevenzione, accertamento e/o perseguimento di frodi;
- g) affermazione, esercizio o difesa di un diritto in sede giudiziaria;
- h) adempimento di un altro specifico obbligo giuridico o contrattuale; ovvero
- i) gestione interna di un'impresa di assicurazioni;
- [j) attività attuariali].

Nascituri

4.5. I dati assicurativi relativi a nascituri dovrebbero essere considerati dati personali e godere di una protezione paragonabile a quella riservata ai dati assicurativi di minori.

Dati sensibili

4.6. La raccolta e il trattamento di dati sensibili dovrebbero essere vietati, a meno che, per uno degli scopi indicati al punto 4.4.:

- a) l'interessato abbia dato esplicitamente il consenso, nella misura in cui ciò non contrasti con le disposizioni del diritto interno; ovvero
- b) ciò sia consentito dalla legge e
 - i) il trattamento sia necessario per l'adempimento di obblighi specifici del titolare; ovvero
 - ii) il trattamento sia necessario per l'affermazione, l'esercizio o la difesa di un diritto in sede giudiziaria;
- c) ciò sia previsto dalla legge, o un'autorità ai sensi del punto 15.1. lo consenta per motivi di rilevante interesse pubblico.

4.7. [Salvo quanto previsto al punto 4.9, i dati genetici non possono essere sottoposti a trattamento per scopi assicurativi]

4.8. [Se il diritto interno lo prevede e offre garanzie adeguate, un assicuratore può, prima di concludere un'assicurazione non obbligatoria, chiedere all'interessato di comunicare i risultati di un'analisi genetica cui si sia già sottoposto, qualora:

- a) i risultati si riferiscano ad una specifica analisi genetica;
- b) siano stati definiti l'affidabilità ed il valore attuariale dei risultati;
- c) la copertura assicurativa sia elevata; e
- d) la conoscenza dei risultati possa limitare la copertura assicurativa offerta].

[La raccolta ed il trattamento di dati genetici sono effettuati da consulenti sanitari, i quali si limitano a trasmettere all'assicuratore le conclusioni ragionate].

4.9. La raccolta ed il trattamento di dati personali relativi a procedimenti penali o condanne penali è consentita unicamente se i dati sono necessari e strettamente connessi a casi di frode, alla concessione di assicurazioni o al pagamento di risarcimenti o altre indennità [e nella misura in cui il trattamento sia conforme a garanzie adeguate previste dal diritto interno].

Marketing diretto

4.10. Se l'interessato ne è stato informato e non vi si è opposto, il titolare dei dati assicurativi può utilizzare i dati raccolti e registrati per scopi assicurativi a fini di marketing e promozione dei propri servizi. Tuttavia, se il trattamento riguarda dati sensibili occorre il consenso esplicito dell'interessato, nella misura in cui ciò non contrasti con norme di diritto interno.

L'interessato deve essere informato del fatto che, qualora rifiuti il consenso o si opponga all'utilizzazione dei propri dati per scopi di marketing, ciò non pregiudica la decisione di concedergli la copertura assicurativa o di consentirgli di continuare a godere della copertura assicurativa già concessa.

Interconnessione

4.11. Il raffronto fra record diversi contenenti dati assicurativi raccolti per la fornitura di specifici contratti assicurativi può essere effettuato unicamente se:

- a) tale raffronto è previsto per legge; ovvero
- b) lo scopo di tale raffronto è compatibile con lo scopo per cui i dati in oggetto sono stati inizialmente raccolti.

5. INFORMAZIONI FORNITE AGLI INTERESSATI

5.1. Gli interessati sono informati di quanto segue:

- a) la o le finalità del trattamento attuale o futuro;
- b) l'identità del titolare dei dati assicurativi;
- c) le categorie di dati raccolti o che si intende raccogliere;
- d) le categorie di persone o enti esterni ai quali essi possono essere comunicati, e per quali finalità;
- e) la possibilità eventuale per l'interessato di rifiutare o ritirare il consenso e le conseguenze in caso di ritiro del consenso;
- f) le condizioni per l'esercizio dei diritti di accesso e di rettifica;
- g) le categorie di altre fonti che possono essere consultate.

5.2. Gli interessati vengono informati di quanto indicato al punto 5.1. al più tardi al momento della raccolta dei dati, a meno che ne siano già stati informati.

Qualora i dati assicurativi non siano raccolti presso l'interessato, quest'ultimo viene informato della raccolta delle informazioni indicate al punto 5.1. non appena i dati sono registrati ovvero, se si prevede di comunicarli a terzi, al più tardi all'atto della prima comunicazione dei dati.

L'obbligo di informare l'interessato non sussiste se:

- a) l'interessato ha già ricevuto le informazioni;
- b) risulta impossibile fornire le informazioni o ciò comporta uno sforzo sproporzionato;
- c) il trattamento o la comunicazione dei dati per scopi assicurativi sono espressamente previsti da norme di diritto interno.

Nei casi di cui alle lettere b. e c., devono essere previste garanzie adeguate.

5.4. Le informazioni da fornire agli interessati devono essere adeguate e adatte alle circostanze. In particolare, le informazioni di cui al punto 5.1., lettere da c. a g., sono fornite all'interessato [unicamente] se ciò risulta necessario per garantire la correttezza della raccolta dei dati.

5.5. Se gli interessati versano in stato di incapacità giuridica e non sono in grado di decidere liberamente, e se le norme di diritto interno non consentono loro di agire per proprio conto, le informazioni devono essere fornite alle persone legalmente autorizzate ad agire per conto dei suddetti interessati. Se un in-

interessato che versa in stato di incapacità giuridica è in grado di comprendere di cosa si tratta, deve essere informato prima della raccolta e del trattamento di dati che lo riguardino.

5.6. Le informazioni fornite agli interessati possono essere limitate se ciò è previsto da norme di legge ed è necessario per la prevenzione o la punizione di un reato penale o per garantire i diritti e le libertà altrui.

6. CONSENSO

6.1. Qualora si chieda agli interessati di prestare il consenso, quest'ultimo deve essere dato liberamente, in modo inequivocabile, specifico e informato. Se il consenso dell'interessato è necessario per la raccolta o il trattamento di dati sensibili, esso deve essere esplicito, libero e informato.

6.2. Qualora i dati assicurativi riguardino persone prive di capacità giuridica che non siano in grado di decidere liberamente, e il diritto interno non consenta all'interessato di agire per proprio conto, è necessario il consenso della persona legalmente autorizzata ad agire nell'interesse dell'interessato, ovvero il consenso di un'autorità o di una persona o ente previsti dalla legge.

6.3. Se, ai sensi del punto 5.5. di cui sopra, un interessato privo di capacità giuridica è stato informato dell'intenzione di raccogliere e trattare dati assicurativi che lo riguardano, se ne dovrebbero tenere in considerazione i desiderata, purché ciò non contrasti con le norme di diritto interno.

7. RACCOLTA E TRATTAMENTO TRAMITE SUBAPPALTO

7.1. In conformità alle norme di diritto interno, il titolare di dati assicurativi può delegare la raccolta ed il trattamento di dati assicurativi per uno scopo specifico, nella misura in cui tale titolare sia autorizzato a raccogliere e trattare i dati in oggetto e il subcontraente si impegni a rispettare le norme di diritto interno che danno attuazione alla presente Raccomandazione, e in particolare a non trattare i dati per scopi diversi.

7.2. I titolari di dati assicurativi devono scegliere subcontraenti che offrano garanzie adeguate per quanto riguarda gli aspetti tecnici e organizzativi del trattamento previsto. Essi devono assicurare l'osservanza di tali garanzie e, in particolare, la conformità del trattamento alle istruzioni impartite.

7.3. La raccolta ed il trattamento di dati da parte di subcontraenti dovrebbero essere regolamentati da un contratto o uno strumento legale che vincoli il subcontraente al titolare dei dati assicurativi e specifichi che il subcontraente agirà esclusivamente nei termini di riferimento indicati dal titolare dei dati assicurativi.

8. COMUNICAZIONE DEI DATI

8.1. I dati assicurativi possono essere comunicati per scopi diversi da quelli previsti al punto 4.4. unicamente se:

a) ciò è previsto da norme di diritto interno per un rilevante interesse pubblico; ovvero

b) gli interessati o i loro legali rappresentanti vi hanno acconsentito in conformità al Capo 6 e nella misura in cui ciò non sia vietato da norme di diritto interno.

9. DECISIONI INDIVIDUALI AUTOMATIZZATE

9.1. Le decisioni in materia assicurativa che hanno conseguenze giuridiche per gli interessati ovvero effetti significativi [soprattutto per quanto riguarda la concessione o l'estensione di un'assicurazione o il pagamento di altre indennità] non sono prese unicamente in base ad un trattamento automatizzato di dati che consenta di categorizzare gli interessati secondo criteri o risultati statistici predefiniti. Tuttavia, tali decisioni possono essere prese se rispondono ad una richiesta avanzata dall'interessato per la conclusione o l'esecuzione di un contratto assicurativo, ovvero se gli interessati hanno la possibilità di esprimere il proprio punto di vista in modo da garantire la tutela dei rispettivi interessi legittimi.

10. DIRITTI DI ACCESSO E RETTIFICA

10.1. Tutti gli interessati devono avere la possibilità di ottenere, su richiesta, tutti i dati che li riguardano, in forma comprensibile, nonché le finalità del trattamento, le categorie di dati interessati dal trattamento, i destinatari o le categorie di destinatari ai quali i dati sono comunicati, e la fonte dei dati. Devono inoltre essere informati, su richiesta, della logica alla base del trattamento automatizzato di dati che li riguardano, almeno in caso di decisioni individuali automatizzate.

10.2. I diritti degli interessati di ottenere i dati che li riguardano non possono essere limitati se non qualora ciò risulti necessario in caso di accertamenti specifici su sospette frodi/abusi assicurativi. In tal caso, l'esercizio del diritto di accesso può essere rimandato al più tardi al termine degli accertamenti.

10.3. Gli interessati hanno il diritto di ottenere la rettifica o la cancellazione dei propri dati assicurativi qualora essi risultino inesatti, non pertinenti, eccessivi o altrimenti raccolti, trattati o registrati in difformità da quanto previsto dalla presente Raccomandazione.

10.4. Ogni rifiuto o limitazione del diritto di accesso e rettifica deve essere motivato per iscritto. I terzi ai quali siano stati comunicati dati assicurativi dovrebbero essere informati delle rettifiche o delle cancellazioni compiute, purché ciò non risulti manifestamente irragionevole o impraticabile.

10.5. I titolari dei dati assicurativi comunicano senza indugio i dati assicurativi pertinenti alle persone che esercitano il diritto di accesso. In linea di principio, il diritto di accesso viene esercitato gratuitamente. Il diritto di accesso non deve mai comportare costi eccessivi.

11. SICUREZZA DEI DATI

11.1. Ogni titolare di dati assicurativi prende le misure tecniche ed organizzative atte a garantire sicurezza, integrità, riservatezza e disponibilità dei dati. Tali misure devono anche proteggere i dati assicurativi dall'accesso, da modifiche e da comunicazioni non autorizzate e da ogni altra forma di trattamento illecito. Queste misure devono essere riesaminate periodicamente.

11.2. Al fine di garantire, in particolare, riservatezza, integrità ed accuratezza dei dati sottoposti a trattamento, nonché la tutela degli interessati, si dovrebbero prendere misure atte a:

a) impedire a persone non autorizzate di accedere ad installazioni utilizzate per il trattamento di dati personali (controllo dell'ingresso alle installazioni);

b) impedire la lettura, la copia, l'alterazione o l'asportazione di supporti informazionali da parte di persone non autorizzate (controllo dei supporti informazionali);

c) impedire l'inserimento non autorizzato di dati nel sistema informativo, ed ogni consultazione, modifica o cancellazione non autorizzate di dati personali sottoposti a trattamento (controllo della memoria);

d) impedire l'utilizzazione di sistemi per il trattamento automatizzato di dati da parte di persone non autorizzate attraverso dispositivi per la trasmissione dei dati (controllo dell'utilizzazione);

e) ai fini, da un lato, dell'accesso selettivo ai dati e, dall'altro lato, della sicurezza dei dati assicurativi, garantire che il trattamento sia strutturato, in linea di massima, in modo da consentire la distinzione fra:

- elementi identificativi e dati relativi all'identità delle persone;
- dati amministrativi
- dati sensibili (controllo dell'accesso);

f) garantire la possibilità di verificare ed accertare a quali persone o enti possono essere comunicati dati personali attraverso dispositivi per la trasmissione dei dati (controllo delle comunicazioni);

g) garantire la possibilità di verificare e determinare *a posteriori* chi abbia avuto accesso al sistema e quali dati personali siano stati inseriti nel sistema informativo, quando e da chi (controllo dell'inserimento dei dati);

h) impedire la lettura, la copia, l'alterazione o la cancellazione non autorizzate di dati personali durante la comunicazione di dati personali ed il trasporto di supporti informazionali (controllo del trasporto);

i) tutelare i dati attraverso la creazione di copie di sicurezza (controllo della disponibilità).

11.3. I titolari di dati assicurativi dovrebbero, in conformità con il diritto interno, definire opportunamente norme interne che rispettino i principi pertinenti contenuti nella presente Raccomandazione.

11.4. Se necessario, i titolari di dati assicurativi dovrebbero nominare una persona indipendente responsabile della sicurezza dei sistemi informativi e della protezione dei dati, con competenze riferite anche alla consulenza sulle materie di cui sopra.

12. FLUSSI TRANSFRONTALIERI DI DATI

12.1. I principi della presente Raccomandazione si applicano ai flussi transfrontalieri di dati assicurativi.

12.2. Il flusso transfrontaliero di dati assicurativi verso uno Stato che abbia ratificato la Convenzione per la protezione delle persone rispetto al trattamento automatico di dati personali, e che disponga di norme legislative le quali offrano una protezione dei dati assicurativi almeno equivalente, non dovrebbe essere soggetto a condizioni particolari per quanto concerne la tutela della riservatezza.

12.3. Se la protezione dei dati assicurativi può essere considerata conforme al principio della protezione equivalente fissato nella convenzione, non dovrebbero essere imposti limiti al flusso transfrontaliero di dati assicurativi verso uno Stato che non abbia ratificato la convenzione, ma disponga di norme legislative le quali prevedono una protezione conforme ai principi della convenzione e della presente Raccomandazione.

12.4. Salvo diversa disposizione del diritto interno, il flusso transfrontaliero di dati assicurativi verso uno Stato che non garantisca una protezione conforme alla convenzione ed alla presente Raccomandazione non dovrebbe di regola effettuarsi, tranne che:

- a) l'interessato abbia dato il proprio consenso, ovvero

b) siano state prese le misure, anche di natura contrattuale, necessarie a rispettare i principi della convenzione e della presente Raccomandazione, e l'interessato abbia la possibilità di opporsi al trasferimento.

[12.5. Tranne in caso di emergenza o in vista di un trasferimento al quale l'interessato abbia dato il proprio consenso conformemente a quanto previsto al Capo 6, dovrebbero essere adottate misure atte a garantire la protezione di dati assicurativi trasferiti da un Paese ad un altro, e in particolare:

a) la persona responsabile del trasferimento dovrebbe indicare al destinatario le specifiche e legittime finalità per le quali i dati sono stati inizialmente raccolti, e le persone o gli enti ai quali essi possono essere comunicati;

b) salvo diversa disposizione del diritto interno, il destinatario dovrebbe impegnarsi con la persona responsabile del trasferimento a rispettare le specifiche e legittime finalità da lui accettate, e a non comunicare i dati a persone o enti diversi da quelli indicati dalla persona responsabile del trasferimento.]

13. CONSERVAZIONE DEI DATI

13.1. Qualora i dati personali non siano più necessari per la realizzazione degli scopi per i quali essi erano stati raccolti e trattati dal titolare, dovrebbero essere distrutti. [Tuttavia, tale cancellazione non deve permettere di eliminare elementi di prova che potrebbero consentire di determinare la responsabilità di compagnie assicurative.] Se i dati devono però essere conservati per scopi di ricerca scientifica o statistica, o per altri scopi previsti dalla legge, essi sono conservati separatamente e possono essere consultati solo per tali scopi, fatta salva l'esistenza di adeguate garanzie.

13.2. Si deve valutare l'opportunità di stabilire un periodo massimo di conservazione dei dati personali qualora sia stata respinta una richiesta di assicurazione. Si deve inoltre tenere conto, nella definizione di un periodo massimo di conservazione, di elementi quali l'esigenza di conservare i dati per il periodo necessario a permettere di far valere un diritto in sede giudiziaria ovvero di fornire la prova di transazioni svolte dall'interessato.

14. MEZZI DI TUTELA

Il diritto interno prevede sanzioni e mezzi di tutela in caso di violazione dei principi stabiliti dalla presente Raccomandazione e recepiti nel diritto interno.

15. GARANTIRE IL RISPETTO DEI PRINCIPI

15.1. Gli Stati membri attribuiscono ad una o più autorità il compito di garantire in piena indipendenza l'applicazione delle disposizioni di diritto interno che danno attuazione ai principi stabiliti nella presente Raccomandazione.

15.2. Le seguenti informazioni devono essere adeguatamente pubblicizzate e facilmente accessibili a tutti:

- a) nominativo e indirizzo del titolare e del suo eventuale rappresentante;
- b) la o le finalità del trattamento;
- c) la categoria o le categorie di interessati e di dati;
- d) il destinatario o le categorie di destinatari ai quali i dati possono essere eventualmente comunicati;
- e) i trasferimenti di dati eventualmente previsti verso Paesi terzi.

5.10.3 Decisione del Consiglio dell'Unione Europea con cui si autorizza la Commissione a negoziare emendamenti alla Convenzione n. 108.

EUROPEAN UNION
THE COUNCIL

Brussels, 10 December 1998

13998/98
LIMITE
ECO 467

«I/A» ITEM NOTE

from: Working Party on Economic Questions (Data Protection)

on: 8 December 1998

to: COREPER/COUNCIL

No. Cion prop.: 10011/98 ECO 247

SUBJECT: Adoption of a Council Decision authorising the Commission to negotiate, within the competent bodies of the Council of Europe, amendments to the Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and recommendations which could be addressed to the Contracting Parties in connection with the application of the Convention

1. On 26 June 1998, the Commission submitted to the Council a recommendation for a Decision authorising the Commission to participate in the above mentioned negotiations.

2. At its meeting on 8 December 1998, the Working Party on Economic Questions (Data Protection) agreed on the text of the Decision as set out in Annex I to this note and certain negotiating directives set out in Annex II.

3. The Permanent Representatives Committee could agree to invite the Council to adopt these texts as an «A» item at one of its forthcoming sessions.

ANNEX I

DRAFT

COUNCIL DECISION

authorising the Commission to participate in the negotiation,
within the competent bodies of the Council of Europe,
of amendments to the Convention of 28 January 1981
for the protection of individuals
with regard to automatic processing of personal data and recommendations
which could be addressed to the Contracting Parties
in connection with the application of the Convention

The Council of the European Union, on a recommendation from the Commission, authorises the Commission to participate, on behalf of the European Community and within the limits of its competence, in the negotiation within the competent bodies of the Council of Europe of amendments to the Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data (hereafter Convention No. 108) and recommendations which could be addressed to the Contracting Parties in connection with the application of Convention No. 108.

The Commission shall conduct the negotiations in cooperation with the special committee appointed by the Council in conformity with the negotiating directives contained in the Annex II.

ANNEX II

NEGOTIATING BRIEF

The negotiations are intended to reach agreement on proposed amendments to Convention No. 108, in the form of a Protocol, in the light of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and in the light of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector.

Possible amendments should be capable of ensuring the free movement of personal data between the European Community and third countries which are Contracting Parties to the amended Convention.

They should add to the current text of the Convention provisions on:

- the establishment by the Contracting Parties of supervisory authorities independently exercising investigative powers, powers of intervention and the power to be party to legal proceedings; and
- the regulation of transfers of personal data from countries which are Contracting Parties to the Convention to countries which are not.

The negotiations also involve proposed recommendation (T-PD 98(14)) which could be addressed to Contracting Parties with regard to the application of the Convention, e.g. in order to encourage them to apply the rules on the protection of individuals to manually processed data intended to form part of the filing system.

5.10.4 Schema degli emendamenti alla Convenzione 108 (T-PD (98) 31)

Strasbourg, 21 September 1998

T-PD (98) 31
Addendum I**Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data (ETS 108).**14th meeting

Strasbourg, 2-4 September 1998

PART A**DRAFT AMENDMENTS TO CONVENTION 108
ALLOWING THE EUROPEAN COMMUNITIES TO ACCEDE****PART B****EXPLANATORY MEMORANDUM
AMENDMENTS TO CONVENTION 108
ALLOWING THE EUROPEAN COMMUNITIES TO ACCEDE**Secretariat memorandum
prepared by the
Directorate of Legal Affairs**DRAFT AMENDMENTS TO CONVENTION 108
ALLOWING THE EUROPEAN COMMUNITIES TO ACCEDE**
prepared, by the Drafting Group of the T-PD, 5-7 March 1998*Article 1*

Paragraphs 2, 3 and 6 of Article 3 of the convention shall read as follows:

«2. Any State or the European Communities may, at the time of signature or when depositing their instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a) that they will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list they shall not include, however, categories of automated data files subject under their domestic law to data protection provisions. Consequently, they shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under their domestic law:

b) that they will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c) that they will also apply this convention to personal data files which are not processed automatically;

3. Any State or the European Communities which have extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State or the European Communities which have made them if they have been made at the time of signature or deposit of their instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.»

Article 2

1. A new paragraph 3, reading as follows, shall be inserted in Article 20 of the convention:

«Every Party has a right to vote. Each State which is a Party to the convention shall have one vote. Concerning questions within their competence, the European Communities exercise their right to vote and cast a number of votes equal to the number of Member States that are Parties to the convention. In this case, the Member States of the Communities do not vote. Conversely, the European Communities do not vote when a question which does not fall within their competence is concerned.»

2. Paragraphs 3 and 4 of Article 20 of the convention shall be renumbered as paragraphs 4 and 5, respectively, of the same article.

Article 3

Article 21, paragraph 2 of the convention shall read as follows:

«Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the European Communities, and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.»

Article 4

Article 23 of the convention shall read as follows:

«Article 23 - Accession by non-member States or the European Communities

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. The European Communities may accede to the convention.

3. In respect of any acceding State, or of the European Communities on accession, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.»

Article 5

Article 24 of the convention shall read as follows:

«Article 24 - Territorial Clause

1. Any State or the European Communities may at the time of signature or when depositing their instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State or the European Communities may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.»

Article 6

Article 27 of the convention shall read as follows:

«Article 27 - Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the European Communities, and any State which has acceded to this convention of:

- a) any signature;
- b) the deposit of any instrument of ratification, acceptance, approval or accession;
- c) any date of entry into force of this convention in accordance with Articles 22, 23 and 24;
- d) any other act, notification or communication relating to this convention.»

PART B

EXPLANATORY MEMORANDUM ON THE AMENDMENTS TO CONVENTION 108 ALLOWING THE ACCESSION OF THE EUROPEAN COMMUNITIES

Introduction and background

1. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter referred to as «the Convention») was opened for signature on 28 January 1981. It entered into force on 1 October 1985.

2. In accordance with Article 18 of the Convention, a Consultative Committee was set up in 1986 and has since reviewed the implementation of the Convention by the Parties, in particular with regard to the economic, technical and political developments in so far as they are of relevance to data protection.

3. Among the important developments of relevance to the Convention was the adoption of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 «on the protection of individuals with regard to the processing of personal data and on the free movement of such data» within the European Communities. The Directive drew much inspiration from the Convention, and aimed at spelling out and expanding on the principles it enshrines. On the basis of the treaties establishing the European Communities, and taking into account in particular the Directive, the European Communities are henceforth empowered to enter into international agreements in the fields it covers. Member States are required to bring into force the laws, regulations and administrative

provisions necessary to comply with this Directive at the latest by 24 October 1998. The provisions were also to be applied to the institutions and organisations of the European Communities.

4. In a letter dated 22 October 1997 the Secretary General of the European Commission notified the Secretary General of the Council of Europe of the application of the Communities to accede to the Convention, and the decision of the Council of the Union, on 22 July 1997, to authorise the Commission to start negotiations with a view to acceding to the Convention as soon as possible. Accession by the Communities reflects the European Union's wish to develop co-operation with the Council of Europe and help create a stronger international forum on data protection, particularly vis-à-vis third countries.

5. As it stands at present, only states may be Parties to the Convention. It was therefore necessary to draft amendments allowing the European Communities to accede.

6. The Consultative Committee drew up the amendments in accordance with Article 21 of the Convention. The Committee of Ministers of the Council of Europe approved them at its ... meeting on ... Following their approval by the Committee of Ministers, the amendments will be submitted to the Parties for acceptance. Under the provisions of Article 21, paragraph 6, of the Convention the amendments will come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof. Following their entry into force, the European Communities will be able to accede to the Convention.

Comments on the amendments

Articles 1, 3, 5 and 6

7. The amendments to Article 3, paragraphs 2, 3 and 6, Article 21, paragraph 2, Article 24 and Article 27 of the Convention are formal amendments, adding the expression «the European Communities» to all the provisions of the Convention which refer only to states.

Article 2

8. The amendment to Article 20 of the Convention aims at regulating voting rights on the Consultative Committee. The new paragraph 3 of Article 20 of the Convention contains a flexible clause taking into account the evolution in the distribution of competences between the European Communities and its member states. It is modelled on similar provisions contained, inter alia, in Article 13.2 of the European Convention for the Conservation of European Wildlife and Natural Habitats (ETS 104, 1979) and Article 20.2 of the European Convention on Transfrontier Television (ETS 132, 1979). Within the Consultative Committee, in the fields of their competence, the European Communities will exercise the right to vote with the same number of votes as the number of their member States which are Parties to the Convention. The European Communities will not be able to exercise the right to vote when the member States vote and conversely.

Article 4

9. The amendment to Article 23 of the Convention contains a provision permitting the European Communities to become a Party to the Convention. It provides for the European Communities to express their consent to be bound by the Convention by way of accession. Accession shall be secured by the deposit of an instrument of accession with the Secretary General of the Council of Europe.

5.10.5 Documento di lavoro 31/98: schema di protocollo aggiuntivo alla Convenzione 108

WORKING DOCUMENT No 31/98

SUBJECT: Community Coordination related to the Protection of Personal Data

At its meeting on 8 December 1998, the Working Group on Economic Questions (Data Protection) examined the draft additional protocol to Convention 108 prepared by the Consultative Committee of Convention 108 (Appendix V of T-PD (98) 31 rev.), in view of the forthcoming drafting group to be held in Strasbourg next February.

The Working Party reached agreement on an amended text which is annexed to this document (English and French version). [Si riporta soltanto la versione inglese]

ANNEX

DRAFT ADDITIONAL PROTOCOL TO CONVENTION 108

Preamble

The Member States of the Council of Europe, and the European Communities, signatories to this Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981 (hereafter referred to as «the Convention»)

Considering a proposal decided upon on ... by the consultative Committee, set up under Article 18 of the Convention, and submitted to the Committee of Ministers, with a view to facilitating or improving the application of the principles of the Convention, in accordance with paragraph a of Article 19,

Convinced that supervisory authorities, exercising their functions with complete independence, are a [...] component of the effective protection of individuals with regard to the processing of personal data,

Considering the importance of the flow of information between people,

Considering that, with the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy, in relation to such exchanges of personal data,

Have agreed as follows:

Article 1

Supervisory authorities

1. Each party shall provide for one or more authorities to be responsible for ensuring compliance, [...] with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention or any additional legal instrument complementary thereto ¹²⁰⁾.

¹²⁰⁾ To be clarified in the explanatory memorandum, the object being to cover only the legally binding texts. Furthermore, the English and French versions differ on this particular point. Therefore it was suggested to reformulate the text in order to make it clearer.

2. To this end, those supervisory authorities shall have in particular powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1.

Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. In accordance with the provisions of Chapter IV and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall cooperate with one another to the extent necessary for the performance of their tasks, in particular by exchanging all useful information.

Article 2

Transfer of personal data towards a country not being party to the Convention

1. Each Party shall provide for the transfer of personal data to a country not being Party to the Convention only if that country ensures an adequate level of protection for the intended data transfer ¹²¹⁾.

2. By way of derogation from paragraph 1 ¹²²⁾, each Party may allow for the transfer of personal data,

a) if domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests or

b) if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer to the competent authorities' satisfaction.

Article 3

Final Provisions

1. As between the Parties, the provisions of Articles 1 and 2 of this Protocol shall be regarded as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

2. This Protocol shall be open for signature by Signatories to the Convention and by the European Communities. It is subject to ratification, acceptance or approval. A Signatory [...] may not ratify, accept or approve this Protocol unless they have previously or are simultaneously ratified, accepted or approved the Convention or have acceded to it. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which ... Signatories of the present protocol have expressed their consent to be bound by the Protocol in accordance with the provisions of Article 3.2.

¹²¹⁾ It was agreed to explain the adequacy of the level of protection in the explanatory memorandum.

¹²²⁾ It was also agreed to explain certain derogations which are laid down in Article 26(2) of the Directive 95/46/EC further in the explanatory memorandum.

In respect of any Signatory [] which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

4. After the entry into force of this Protocol, any State or the European Communities which has acceded to the Convention may also accede to this Protocol.

Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

5. Any Party may at any time denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

6. The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the European Communities and any other State which has been invited to accede to the Convention of:

- a) any signature;
- b) the deposit of any instrument of ratification, acceptance, approval or accession;
- c) any date of entry into force of this Protocol in accordance with Article 3;
- d) any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at ..., this ... day of ..., in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, the European Communities and to any State invited to accede to the Convention.

5.11 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ECONOMIQUES

5.11.1 Conferenza ministeriale di Ottawa: 7-9 ottobre 1998

Non classifié

SG/EC(98)14/FINAL

Organisation de Coopération et de Développement Economiques OLIS: 18-Dec-1998

Organisation for Economic Co-operation and Development Dist.: 22-Dec-1998

Or. Ang.

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE COMITÉ DE PILOTAGE POUR LA PRÉPARATION DE LA CONFÉRENCE MI- NISTÉRIELLE D'OTTAWA «UN MONDE SANS FRONTIÈRES: CONCRE- TISER LE POTENTIEL DU COMMERCE ÉLECTRONIQUE MONDIAL»

CONFÉRENCE MINISTÉRIELLE DE L'OCDE
«UN MONDE SANS FRONTIÈRES: CONCRETISER LE POTENTIEL
DU COMMERCE ÉLECTRONIQUE MONDIAL»
OTTAWA, 7-9 OCTOBRE 1998

CONCLUSIONS DE LA CONFÉRENCE

73016

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

AVANT PROPOS

Le présent document contient les conclusions de la Conférence ministérielle d'Ottawa des 7-9 octobre 1998. Les trois déclarations ministérielles adoptées par la Conférence, Déclaration des ministres relative à la protection de la vie privée sur les réseaux [DSTI/ICCP/REG(98)10/REV2], Déclaration sur la protection des consommateurs dans le contexte du commerce électronique [DSTI/CP(98)12/REV2], Déclaration ministérielle sur l'authentification pour le commerce électronique [DSTI/ICCP/REG(98)9/REV4], figurent en annexe. Le Conseil a adopté, au cours de sa 934^{ème} session tenue le 19 octobre 1998, une résolution intégrant ces trois Déclarations dans les instruments de l'OCDE.

Les textes de ces trois Déclarations ont été mis en diffusion générale sous des cotes /FINAL.

Copyright OCDE, 1998

**Les demandes de reproduction ou de traduction doivent être adressées à:
M. le Chef du Service des Publications, OCDE, 2 rue André-Pascal, 75775
Paris Cedex 16, France.**

CONCLUSIONS DE LA CONFERENCE

Les Ministres de l'OCDE, des observateurs de pays non membres de l'OCDE, des dirigeants d'organisations internationales, des chefs d'entreprises et des représentants des syndicats, des consommateurs et groupes d'intérêts sociaux se sont réunis à Ottawa du 7 au 9 octobre 1998, afin d'assembler leurs plans de soutien au développement du commerce électronique mondial. Cette Conférence ministérielle de l'OCDE, accueillie par le Gouvernement du Canada et qui a été présidée par l'honorable John Manley, Ministre de l'industrie du Canada, représente une étape importante dans l'élaboration d'un plan mondial pour le commerce électronique transnational.

Du point de vue de l'OCDE la Conférence d'Ottawa a fait oeuvre de pionnier sur un certain nombre de plans. Pour la première fois, lors d'une réunion ministérielle, les pays Membres de l'OCDE ont fait appel à la participation active d'organisations internationales, du secteur privé, du milieu syndical, du monde de la consommation et des groupes d'intérêts sociaux dans un effort ouvert et transparent pour examiner les éléments du commerce électronique mondial. Autre première à l'occasion d'une Conférence ministérielle de l'OCDE, une exposition organisée par l'industrie a permis d'illustrer les applications pratiques destinées à répondre aux grandes questions discutées pendant la Conférence.

Par définition, le commerce électronique a une envergure mondiale. Que les mesures prises soient de nature nationale ou régionale, privée ou publique, toutes les politiques et les activités relatives au commerce électronique n'auront que des effets limités si elles ne vont pas dans le sens d'une approche mondiale. En convoquant la Conférence d'Ottawa, les gouvernements des pays de l'OCDE ont reconnu l'importance de la collaboration entre les gouvernements comme avec les entreprises, les travailleurs et les consommateurs pour le développement et l'utilisation du commerce électronique, ainsi que la nécessité pour son application d'une démarche de coopération dans tous les secteurs et au-delà des frontières nationales. A cette fin, les Ministres de l'OCDE, le Comité consultatif économique et industriel auprès de l'OCDE (BIAC), la Commission syndicale consultative auprès de l'OCDE (TUAC), et les autres participants du secteur privé ont conclu que:

- le commerce électronique offre un moyen fondamentalement nouveau d'effectuer des transactions commerciales, et peut constituer un moyen important de stimulation de la croissance économique, et du renforcement du développement dans le monde entier;
- les politiques élaborées dans tous les pays et enceintes internationales pour faciliter le développement du commerce électronique mondial doivent encourager la coopération entre tous les acteurs concernés (gouvernements, consommateurs, entreprises, syndicats et institutions publiques) ainsi que le dialogue social, et leurs actions doivent être dans toute la mesure du possible compatibles à l'échelon international;
- les gouvernements doivent promouvoir un environnement favorable à la concurrence pour permettre au commerce électronique de s'épanouir, s'efforcer de réduire et d'éliminer les obstacles injustifiés aux échanges, et agir, lorsque

cela est nécessaire, pour assurer dans l'espace numérique comme dans l'espace physique, une protection adéquate des objectifs d'intérêt public essentiels;

- l'intervention gouvernementale, lorsqu'elle s'avère nécessaire, devrait être proportionnée, transparente, cohérente et prévisible, et neutre sur le plan technologique;

- les gouvernements devraient reconnaître l'importance d'une coopération suivie entre les entreprises pour l'établissement des normes et le renforcement de l'interopérabilité dans un cadre international, volontaire et consensuel;

- le secteur privé devrait continuer à jouer un rôle clé dans le développement et la mise en oeuvre de solutions à un certain nombre de questions essentielles pour le développement du commerce électronique, tout en reconnaissant et en prenant en compte les objectifs fondamentaux qui s'appliquent sur les plans économique, social et de l'intérêt public, et en travaillant en étroite liaison avec les gouvernements et tous les acteurs concernés.

A partir de leurs échanges de vues, les participants à la Conférence ont dégagé des éléments menant à une vision partagée du commerce électronique mondial. Dans ce contexte, les participants ont discuté des priorités relatives au secteur privé, au milieu syndical et à l'intérêt du public, des recommandations des Ministres à l'égard des priorités et futurs travaux de l'OCDE, ainsi que des travaux importants actuellement en cours au sein des organismes internationaux.

Une vision commune du commerce électronique mondial

La Conférence a réaffirmé que la rapidité du développement et de l'expansion du commerce électronique mondial nécessitera une approche vaste et concertée de la part des pouvoirs publics, du secteur privé et des organisations internationales, en vue de favoriser un environnement stable et prévisible qui facilitera sa croissance et en maximisera le potentiel socio-économique dans l'ensemble des sociétés et des économies. A cet égard, les participants ont convenu que pour faciliter le commerce électronique mondial, il importe de s'attaquer aux questions qui se posent en relation avec les quatre thèmes suivants.

1. Renforcer la confiance des utilisateurs et des consommateurs

Le marché numérique doit gagner la confiance des utilisateurs. Le cadre et les garanties réglementaires qui assurent cette confiance sur le marché traditionnel doivent être, le cas échéant, adaptés afin de susciter une confiance durable sur le marché numérique. Les gouvernements ont dans ce contexte une responsabilité fondamentale. En même temps, on attend beaucoup du rôle moteur du secteur privé et beaucoup de choses en dépendent. Les participants ont souligné les domaines essentiels où il importe d'agir pour stimuler la croissance et l'utilisation du commerce électronique: la création et mise en oeuvre de technologies et de politiques dignes de confiance; le cas échéant, le développement de réglementations de base; et le développement de codes de conduite, de normes, de schémas d'organisation industrielle et institutionnelle, et d'outils technologiques nécessaires à l'autorégulation» ainsi qu'à la protection effective des consommateurs et à l'habilitation des utilisateurs dans différents environnements.

2. Etablir les règles fondamentales régissant le marché numérique

Au moment où les gouvernements, l'industrie et les consommateurs s'aventurent dans ce nouveau domaine, ils cherchent à s'assurer qu'une protection effective est offerte sur le marché numérique, et que l'on s'attaque aux obstacles injustifiés au commerce électronique. Des cadres juridiques ne devraient être mis en place que là où ils sont nécessaires, ils devraient favoriser un environnement concurrentiel, et ils devraient être clairs, cohérents et prévisibles.

3. Améliorer l'infrastructure de l'information pour le commerce électronique

L'expansion du commerce électronique repose sur l'accès universel et abordable à l'infrastructure de l'information. La concurrence effective sur les marchés des télécommunications peut assurer une évolution durable à long terme vers l'abaissement des coûts, l'accroissement de la qualité, et par là l'élargissement de l'accès aux infrastructures et services d'information. Les participants à la Conférence ont reconnu qu'il importe de s'attaquer adéquatement au Problème de l'an 2000.

4. Optimiser les avantages

Le passage à une économie numérique est un élément important de l'évolution plus générale vers une société mondiale de l'information. Le potentiel économique et social du commerce électronique ne se concrétisera pleinement que par son utilisation généralisée par les entreprises, les consommateurs et les institutions publiques. L'Etat, en tant qu'utilisateur modèle des technologies existant sur le marché, peut constituer un moteur essentiel dans la création d'un marché électronique. Une modernisation et une adaptation réussies des organisations, ainsi que les compétences et les connaissances des citoyens sont des éléments importants de stimulation de l'utilisation du commerce électronique. Sa croissance exige aussi une main d'oeuvre motivée et hautement qualifiée. Il est nécessaire d'avoir une compréhension claire des incidences sociales et économiques, y compris des répercussions sur la croissance, la productivité et l'emploi, ainsi que des besoins des entreprises et notamment des petites et moyennes entreprises, des organisations et des consommateurs dans les pays aussi bien en développement que développés.

Traduire la vision dans la réalité

Trois documents clés donnant les grandes lignes des activités actuelles et futures relatives au commerce électronique (documents ci-joints) ont été soumis à la Conférence:

- le *Plan d'action de l'OCDE pour le commerce électronique* qui présente ses activités et des recommandations pour ses futurs travaux;
- le *Rapport sur les organismes internationaux et régionaux: activités et initiatives relatives au commerce électronique* qui présente les travaux actuels et potentiels de ces organismes;
- un *plan d'action global préparé par l'industrie du commerce électronique avec des recommandations pour les gouvernements* qui présente les initiatives actuelles du secteur privé et ses vues sur les questions clés.

Les participants se sont félicités de ces efforts significatifs vers une collaboration mondiale et une compatibilité accrue des approches à l'égard du commerce électronique dans le secteur privé, les organisations internationales et régionales, ainsi qu'à l'OCDE.

Les participants à la Conférence ont réaffirmé le rôle que jouent les gouvernements dans la création pour le commerce électronique mondial, d'un environnement où les règles fondamentales sont appropriées, claires et prévisibles, et où la collaboration entre tous les acteurs est facilitée au niveau mondial. Ils ont également noté que les gouvernements ont pour responsabilité de préserver l'intérêt public. Les participants à la Conférence ont pris note de l'accord auquel sont parvenus les Ministres, qui figure ci-dessous.

Les travaux de l'OCDE Accord des Ministres de l'OCDE

«Les Ministres de l'OCDE ont réaffirmé l'importance de la contribution qu'apportent les travaux de l'OCDE au développement mondial du commerce électronique, ils ont recommandé que soient entrepris les travaux présentés dans le «Plan d'action de l'OCDE pour le commerce électronique» et ils ont demandé au Secrétaire général et au Conseil de l'OCDE que ce Plan d'action reçoive une priorité élevée dans le programme de travail de l'OCDE, en tenant compte des compétences de ses organes subsidiaires et du niveau des ressources disponibles. Les Ministres ont attaché une importance particulière aux travaux de l'OCDE portant sur la fiscalité, la protection de la vie privée, la protection des consommateurs, l'authentification, les infrastructures et les conséquences socio-économiques, et ont en même temps pris note des travaux menés dans les autres domaines du Plan d'action. Les Ministres ont pris note des rapports de référence «Le rôle des infrastructures de télécommunication et d'information dans l'avancement du commerce électronique», «Les incidences économiques et sociales du commerce électronique: Résultats préliminaires et programme de recherche», et «Le problème de l'an 2000: Incidences et actions». Les Ministres ont aussi demandé à l'OCDE de faire en sorte que ses travaux soient dans toute la mesure du possible menés de façon coordonnée avec les autres organisations internationales, l'industrie, les ONG, et soient diffusés aussi largement que possible à la communauté mondiale.

«Les Ministres de l'OCDE ont affirmé qu'ils ont l'intention de travailler ensemble, et en partenariat avec le secteur privé et les organisations sociales pour créer la confiance dans le marché numérique, clarifier les règles, renforcer l'accès aux infrastructures en mettant en place un marché des télécommunications libéralisé et concurrentiel, et maximiser les bénéfices pour tous les citoyens. A cette fin ils ont:

- adopté une Déclaration relative à la protection de la vie privée sur les réseaux mondiaux (ci-jointe) qui réaffirme leur engagement à l'égard d'une protection effective de la vie privée sur les réseaux mondiaux, affirme leur détermination à prendre les mesures nécessaires à cette fin, et reconnaît la nécessité de coopérer avec l'industrie et les entreprises; conformément aux termes de la Déclaration, ils ont également convenu que l'OCDE devrait fournir des orientations pratiques pour la mise en oeuvre des lignes directrices de l'OCDE sur la protection de la vie privée en s'inspirant de l'expérience et des exemples nationaux;*

- adopté une Déclaration sur la protection des consommateurs dans le contexte du commerce électronique (ci-jointe) qui reconnaît que les gouvernements, l'industrie et les représentants doivent continuer à travailler ensemble pour faire en sorte que les consommateurs bénéficient d'un niveau de protection transparent*

et efficace, et qui invite instamment l'OCDE à achever ses travaux en cours pour rédiger en 1999 de véritables «Lignes directrices sur la protection des consommateurs dans le contexte du commerce électronique»;

– adopté une Déclaration sur l'authentification pour le commerce électronique (ci-jointe) qui reconnaît l'importance de l'authentification pour le commerce électronique et indique un certain nombre d'actions propres à promouvoir le développement des technologies et mécanismes d'authentification, notamment la poursuite des travaux menés au niveau international avec le secteur privé, l'industrie, et les représentants des utilisateurs;

– se sont félicités du rapport «Conditions cadres pour l'imposition du commerce électronique» qui énonce les principes qui devraient s'appliquer à l'imposition du commerce électronique et présente les conditions cadres d'imposition sur lesquelles existe un accord, et ils ont approuvé les propositions que contient ce rapport pour poursuivre les travaux.

«Les Ministres ont aussi reconnu l'importance de la confiance des consommateurs et des investisseurs dans le commerce électronique pour assurer sa croissance future. Ils ont noté que les dirigeants des entreprises et les différents groupes industriels ont l'intention d'élaborer des cadres d'autorégulation pour le commerce électronique. Les Ministres ont souligné que lorsqu'on utilise des mécanismes d'autorégulation, ils devraient être transparents, non discriminatoires et ouverts à tous les acteurs du marché, et ils ont encouragé le secteur privé à agir rapidement pour répondre aux attentes du public dans ces domaines.»

Activités et initiatives des organisations internationales

Bon nombre d'organismes régionaux et d'organisations internationales ont entrepris des travaux qui affectent directement ou indirectement la croissance du commerce électronique. Ces travaux couvrent notamment les normes techniques volontaires et élaborées par consensus, la libéralisation des échanges, l'assistance technique, la mise en oeuvre et le suivi des politiques, ainsi que des examens et des analyses.

Le *Rapport sur les organismes internationaux et régionaux: activités et initiatives relatives au commerce électronique*, qui est fondé sur les contributions d'un grand nombre d'organisations internationales et régionales sous leur propre responsabilité, représente la première compilation des réalisations, ainsi que des travaux en cours ou en projet de ces organismes internationaux. La Conférence s'est félicitée de cette initiative de collaboration entre organisations, et a grandement apprécié les efforts faits pour créer cet aperçu complet des activités relatives au commerce électronique.

Les participants à la Conférence ont reconnu le rôle primordial du secteur privé pour stimuler la croissance du commerce électronique mondial grâce à l'investissement et au dynamisme de l'innovation de produits et de services, ainsi que la nécessité du partenariat entre les gouvernements et le secteur privé pour obtenir la confiance et l'acceptation des consommateurs. Dans ce contexte, les participants à la Conférence ont pris note des priorités du secteur privé qui figurent ci-dessous.

Priorités du secteur privé

«Un groupement d'organisations industrielles internationales a été coordonné par le Comité consultatif économique et social (BIAC); il comprend La Commission de l'infrastructure globale de l'information (GIIC), la Chambre de commerce interna-

tionale (CCI), le Groupe international des usagers des télécommunications (CCI), l'Organisation mondiale pour les technologies et services informatiques (WITSA), en coopération avec le Forum sur les règles et les droits relatifs à Internet (ILPF). Ce groupement, avec le soutien d'un ensemble d'autres organisations internationales, régionales ou spécialisées, a soumis à la Conférence «Un plan d'action global préparé par l'industrie du commerce électronique avec des recommandations pour les gouvernements». Ce plan d'action expose entre autres que:

- le développement du commerce électronique devrait être laissé principalement à l'initiative du secteur privé en réponse aux forces du marché, et les gouvernements devraient reconnaître et renforcer ce rôle;*
- le secteur privé continuera à développer l'autorégulation et l'innovation technologique pour stimuler l'habilitation des utilisateurs, conformément à la loi dans la mesure de son applicabilité;*
- le gouvernement et l'industrie ont l'un et l'autre un rôle approprié à jouer;*
- les politiques de soutien au commerce électronique et à la convergence des télécommunications, des technologies de l'information et du secteur des multimédias, devraient être mises en oeuvre dans un environnement ouvert et concurrentiel.*

«Le secteur privé accroît la protection de la vie privée par l'autorégulation, par des codes volontaires, par des dispositions contractuelles types, et en offrant des technologies disponibles sur le marché qui permettent un niveau élevé de protection de la vie privée ajusté aux besoins et aux préférences des utilisateurs. A partir de son expérience du marché mondial, il continue à développer en matière d'information des pratiques équitables qui sont en cohérence avec les Lignes directrices de l'OCDE sur la vie privée de 1980, et il aide les utilisateurs à développer les qualifications dont ils ont besoin pour se protéger et faire des choix dans un environnement en ligne.

«Le secteur privé améliore des outils sophistiqués conçus pour protéger et habiliter les consommateurs sans réglementation gouvernementale excessive, et il participe, avec les gouvernements et les autres parties intéressées, aux discussions internationales visant à développer des approches pour la protection des consommateurs.

«En ce qui concerne l'authentification pour le commerce électronique, le secteur privé s'efforce d'assurer l'interopérabilité technique, de promouvoir l'acceptabilité juridique des certificats et signatures électroniques aux niveaux national et international, et de contribuer à développer, avec les gouvernements dans le cadre de la CNUDCI, les cadres juridiques appropriés pour assurer prédictibilité et certitude.

«Pour la fiscalité, le secteur privé continue à travailler avec l'OCDE pour assurer que la neutralité constitue le principe directeur, et que les taxes ne sont pas imposées de façon discriminatoire.

«Pour appuyer ces initiatives, le secteur privé:

- développe des procédures transparentes pour la protection des informations de caractère personnel;*
- développe, à partir de l'expérience du marché mondial, des lignes directrices et des normes commerciales pour les fournisseurs d'accès à Internet et les opérateurs de site sur la Toile; met en place des mécanismes internationaux appropriés d'application par autorégulation pour les cas de violation des règles exemplaires relatives à la publicité et la recherche de marchés interactives;*

- continue de développer des normes et codes de conduite acceptés au niveau international, ainsi que des répertoires centraux d'informations pertinentes pour les entreprises (par exemple, au sujet des pratiques de certification); et
- travaille par l'intermédiaire de leurs gouvernements avec l'OMC pour promouvoir un calendrier d'engagements significatifs de libéralisation des télécommunications de la part de tous ses états membres.»

Les participants à la Conférence ont reconnu que tout un ensemble d'intérêts sociaux doivent être inclus et impliqués dans les efforts visant à faciliter la croissance du commerce électronique mondial. La participation à la Conférence de représentants des syndicats, des consommateurs et d'autres groupes non gouvernementaux témoigne de l'importance du commerce électronique dans l'évolution de la vie sociale, civique et communautaire. Dans ce contexte, les participants à la Conférence ont pris note des vues sur les perspectives sociales présentées par les organisations syndicales, les organisations de consommateurs et les organisations non gouvernementales ci-dessous.

Perspectives sociales

«La Commission syndicale consultative (TUAC) et les représentants des groupes d'intérêt public se sont réunis lors d'une séance parallèle de la Conférence afin d'étudier les perspectives sociales. La Conférence a permis de reconnaître et de confirmer le rôle, la place et la participation des groupes d'intérêt public à l'égard des discussions et négociations internationales actuelles sur le commerce électronique. Le document d'étude « *Electronic Commerce Developments and Challenges* » de la Commission et la lettre des représentants des groupes d'intérêt public aux ministres de l'OCDE et des autres pays présents à la Conférence ministérielle d'Ottawa (qui est considérée comme un document de la Conférence, disponible en s'adressant à l'OCDE) décrivent leurs vues sur cette question.

«Les représentants des organisations syndicales, des organisations de consommateurs et des autres organisations non gouvernementales participant à la Conférence, coordonnées par la Commission syndicale consultative auprès de l'OCDE (TUAC), ont reconnu l'importance du commerce électronique dans l'évolution de la vie sociale, civique et communautaire, ainsi que sa contribution essentielle au changement économique et social. Ils ont donc appelé les gouvernements et le secteur privé à inclure tout l'éventail des intérêts de la société dans leurs efforts pour promouvoir la diffusion du commerce électronique.

«Au cours de leur session, les représentants des organisations syndicales, des organisations de consommateurs et des autres organisations non gouvernementales ont identifié pour les travaux actuels et futurs plusieurs domaines qu'ils considèrent comme essentiels pour la pleine réalisation du potentiel économique et social du commerce électronique.

«Améliorer l'accès, les qualifications et la «culture numérique»» - L'ampleur et l'intensité de l'utilisation des réseaux de télécommunications est un des premiers facteurs déterminants de l'application à grande échelle du commerce électronique et de la construction en cours d'une société de l'information. Les représentants des organisations syndicales et des organisations de consommateurs ont donc souligné la nécessité d'efforts des gouvernements et de l'industrie pour accroître la «culture numérique», l'éducation et la formation. En outre ils ont signalé qu'un accès abordable aux réseaux numérique est essentiel si

l'on veut diffuser largement les bénéfices du commerce électronique dans l'économie et la société, et ainsi éviter une séparation entre «riches» et «pauvres» en information.

«Vie privée, confiance et contenu - Afin de garantir une large acceptation du marché numérique les représentants des organisations syndicales et des autres groupes d'intérêts sociaux ont considéré qu'il est extrêmement important de résoudre de façon suffisante les questions qui se posent actuellement dans les domaines de la vie privée des consommateurs et des employés, de la protection des consommateurs (sécurité des paiements, fiabilité des entreprises, réparation, etc.) et de la diffusion de contenu offensif et préjudiciable. Ils ont exprimé leur soutien aux efforts visant à minimiser la collecte de données de caractère personnel et à maximiser la protection de la vie privée des individus. Ils ont en outre appelé les gouvernements, le secteur privé et les ONG à travailler ensemble pour renforcer le cadre nécessaire à une protection effective des consommateurs et de la vie privée, fondée sur un cadre de réglementation légale, de codes de conduite et d'applications technologiques appropriées.

«Conséquences sociales, coûts et bénéfices - Le commerce électronique va entraîner une extension géographique des marchés et à la création de nouvelles entreprises. Ce processus comportera la création d'un certain nombre d'emplois nouveaux et qualifiés. Mais en même temps le changement sera aussi marqué par l'élimination d'emplois. Le commerce électronique aura donc des effets sur l'ensemble du secteur privé, de l'économie et de la société. Pour faire face aux conséquences sociales, pour éviter ou réduire les risques et pour garantir une large distribution des bénéfices favorable à la justice sociale et à la qualité de la vie, les représentants des organisations syndicales et des organisations de consommateurs ont souligné la nécessité de prendre en considération dans son ensemble la relation mutuelle entre société et technologie.

Greffer le commerce électronique dans les structures organisationnelles - L'application des réseaux de télécommunication et des technologies de l'information au niveau de la firme est un instrument puissant d'accroissement de la productivité et de la compétitivité. Toutefois, pour l'appropriation ces bénéfices, les représentants des organisations syndicales ont appelé de leurs vœux une approche intégrée combinant l'introduction des technologies et une réorganisation du travail, telle que la décrivent les rapports de l'OCDE sur Technologie, productivité et création d'emplois. Ils ont en outre considéré que la participation des employés au processus d'extension du travail d'équipe, de simplification des hiérarchies et de développement des compétences est une précondition essentielle de la maximisation du potentiel du commerce électronique.

Combiner flexibilité et sécurité - Les technologies de l'information et les réseaux de télécommunications offrent une flexibilité de la gestion du temps et de la localisation du travail qui ouvre de nouvelles possibilités pour les entreprises et les employés. En même temps, ces nouvelles options adressent des défis aux systèmes de sécurité sociale et de relations industrielles, aux acteurs de ces systèmes, et au cadre politique au sein duquel ils agissent. Pour assurer que les coûts et les bénéfices de la flexibilité seront distribués équitablement, les participants de la Session des organisations syndicales et des ONG ont reconnu le besoin d'une mise à jour des systèmes réglementaires de façon à ce qu'ils intègrent les nouvelles formes de travail et contribuent à la cohésion sociale.

«Pour les représentants des organisations syndicales et des organisations de consommateurs, un commerce électronique véritablement «mondial» exige un cadre international de coopération qui maximise la possibilité de bénéfices pour toutes les composantes de la société et évite le risque d'un ajustement à la baisse du bien-être social, des conditions de travail et des niveaux de vie. A cet égard, les participants à la conférence représentant les organisations syndicales, les organisations de consommateurs et les ONG se sont félicités des travaux entrepris pour examiner les effets économiques et sociaux du commerce électronique et plus généralement des technologies de l'information. Ils ont examiné la nécessité d'une poursuite de ces travaux pour élargir et intensifier les incitations aux recherches concernant en priorité les incidences sur l'emploi, le cadre de travail et la qualité de la vie.

«Les participants à la conférence représentant les organisations syndicales, les organisations de consommateurs et les ONG estiment qu'il y a un besoin durable de participation des groupes d'intérêts sociaux à l'évolution future du commerce électronique. Ils considèrent que cette participation est un complément nécessaire des responsabilités législatives et politiques des gouvernements et du rôle du secteur privé dans la création d'innovation, d'investissement et d'emploi. Ils sont prêts à être les partenaires des gouvernements et du secteur privé dans les efforts visant à assurer une évolution socialement acceptable vers une économie numérique. A leur avis, la Conférence d'Ottawa représente une étape importante vers l'instauration d'un dialogue continu entre les organisations non gouvernementales et intérêts sociaux, le secteur privé et le gouvernements, et ils chercheront à recommencer ce dialogue et à s'appuyer sur ces fondations pour édifier la future société de l'information.»

Prochaines étapes Concrétiser le potentiel

Cette Conférence, qui fait suite à la Conférence de Turku de l'OCDE et à d'autres conférences régionales et internationales, constitue une étape importante de la concrétisation du potentiel du commerce électronique mondial, de la promotion de la coopération mondiale, et de la mise en place des éléments du développement futur de la société mondiale de l'information. Les participants ont reconnu que dans un environnement mondial en évolution rapide, il est nécessaire que tous collaborent dans le sens des objectifs de la Conférence: renforcer la confiance des utilisateurs et des consommateurs; établir les règles fondamentales du marché numérique; améliorer l'infrastructure de l'information sur laquelle reposera le commerce électronique; optimiser les avantages que procurera à tous le commerce électronique mondial.

La Conférence d'Ottawa est une étape marquante de l'évolution vers un commerce électronique mondial, et a dégagé des opportunités de travaux futurs. La Conférence a fait avancer le processus en créant au niveau mondial une meilleure compréhension du commerce électronique, qui contribuera à une plus grande compatibilité internationale des politiques afin de permettre à toutes les économies de maximiser les possibilités qu'offre cette nouvelle plate-forme numérique. Les plans d'action de l'OCDE et du secteur privé, de même que le rapport sur les activités et initiatives des organisations internationales, indiquent comment les différents acteurs concernés ont l'intention de contribuer à la future coopération mondiale en matière de commerce électronique.

Les participants à la Conférence ont fait ressortir la nécessité d'une coopération durable et efficace, et d'échanges réguliers d'information au sein des pouvoirs publics et entre ces derniers, les différentes industries, le secteur privé, les consommateurs, les groupes de défense de l'intérêt public, les pouvoirs publics et les organes internationaux.

À cette fin, en plus des travaux en cours de l'OCDE et de son Plan, les délégués à la Conférence ont exhorté l'OCDE à:

- utiliser ses compétences en matière de recherche et de statistiques pour analyser et mesurer les incidences économiques et sociales du commerce électronique mondial;

- rendre compte régulièrement à la collectivité mondiale des progrès réalisés à l'échelon national et international pour faire du commerce électronique mondial une réalité, et ce, en apportant des solutions aux quatre grandes questions de politique que comportent les thèmes de la conférence: «Renforcer la confiance des confiances des utilisateurs et des consommateurs», «Etablir les règles fondamentales régissant le marché numérique», «Améliorer l'infrastructure de l'information», et «Optimiser les avantages»;

- travailler de concert avec d'autres organisations internationales et organismes régionaux, avec le secteur privé, et avec les pays non membres de l'OCDE en vue de favoriser la collaboration et la coordination au sein du plus grand nombre d'enceintes possibles comme entre ces différentes enceintes, et faire ainsi progresser le commerce électronique mondial.

ANNEXE 1

DECLARATION RELATIVE A LA PROTECTION DE LA VIE PRIVEE SUR LES RESEAUX

qui a été formulée par les Ministres de l'OCDE
à la Conférence «Un monde sans frontières:
concrétiser le potentiel du commerce électronique mondial»
7-9 octobre 1998, Ottawa, Canada

Les Gouvernements des pays Membres de l'OCDE ¹²³⁾ :

Considérant que le développement et la diffusion à l'échelle mondiale des technologies numériques de l'informatique et des réseaux présentent des avantages sociaux et économiques en encourageant les échanges d'informations, en élargissant le choix offert aux consommateurs, et en favorisant l'expansion des marchés et l'innovation de produits;

Considérant que les technologies des réseaux mondiaux facilitent l'expansion du commerce électronique et accélèrent le développement des communications et des transactions électroniques transfrontières entre gouvernements, entreprises, utilisateurs et consommateurs;

Considérant que le recueil et la manipulation de données de caractère personnel devraient s'effectuer dans le dû respect de la vie privée;

¹²³⁾ incluant les Communautés européennes

Considérant que les technologies numériques de l'informatique et des réseaux améliorent les méthodes traditionnelles de traitement des données de caractère personnel, augmentent l'aptitude à collecter, rassembler et rapprocher d'importantes quantités de données et à produire des informations enrichies et des profils de consommateurs;

Considérant que les technologies numériques de l'informatique et des réseaux peuvent aussi être utilisées pour instruire les utilisateurs et les consommateurs des problèmes de protection de la vie privée en ligne, et pour les aider à préserver leur anonymat dans des circonstances appropriées ou à exercer leur liberté de choix eu égard aux utilisations qui sont faites de leurs données personnelles;

Considérant que pour accroître la confiance dans les réseaux mondiaux, les utilisateurs et consommateurs ont besoin d'avoir des assurances quant au caractère loyal de la collecte et du traitement des données personnelles les concernant, notamment des données relatives à leurs activités et transactions en ligne;

Considérant que des mesures sont nécessaires pour assurer la protection efficace et généralisée de la vie privée par les entreprises qui collectent ou traitent des données de caractère personnel, de manière à accroître la confiance des utilisateurs et consommateurs dans les réseaux mondiaux;

Considérant que des règles et règlements transparents régissant la protection de la vie privée et des données de caractère personnel et leur mise en oeuvre efficace sur les réseaux d'information sont un élément clé pour accroître la confiance dans les réseaux mondiaux;

Considérant que des approches différentes et efficaces élaborées, en matière de protection de la vie privée, par les pays Membres, notamment l'adoption et la mise en oeuvre de lois ou de dispositifs d'autorégulation par l'industrie, peuvent se combiner pour parvenir à un niveau efficace de protection de la vie privée sur les réseaux mondiaux;

Considérant le besoin de coopération mondiale, et la nécessité que le secteur industriel et commercial joue un rôle majeur, en concertation avec les consommateurs et les pouvoirs publics, pour assurer la mise en oeuvre efficace des principes de protection de la vie privée sur les réseaux mondiaux;

Considérant que les principes technologiquement neutres énoncés dans les Lignes directrices de l'OCDE sur la protection de la vie privée de 1980 continuent de refléter un consensus international sur les orientations qui doivent guider la collecte et la manipulation des données de caractère personnel sur quelque support que ce soit, et fournissent une base sur laquelle fonder la protection de la vie privée sur les réseaux mondiaux;

RÉAFFIRMATION des objectifs énoncés dans

La Recommandation concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptée par le Conseil de l'OCDE le 23 septembre 1980 (Lignes directrices de l'OCDE sur la protection de la vie privée);

La Déclaration sur les flux transfrontières de données, adoptée par les Gouvernements des pays Membres de l'OCDE le 11 avril 1985; et

La Recommandation relative aux Lignes directrices régissant la politique de cryptographie, adoptée par le Conseil de l'OCDE le 27 mars 1997.

DÉCLARENT

Qu'ils vont réaffirmer leur engagement à l'égard de la protection de la vie privée sur les réseaux mondiaux, afin d'assurer le respect de droits importants, de construire la confiance dans les réseaux mondiaux et d'empêcher des restrictions inutiles aux flux transfrontières de données de caractère personnel;

Qu'ils s'attacheront à établir des passerelles entre les différentes approches adoptées par les pays Membres en vue de garantir la protection de la vie privée sur les réseaux mondiaux sur la base des Lignes directrices de l'OCDE;

Qu'ils prendront, dans le cadre de leurs lois et pratiques respectives, les mesures nécessaires pour garantir la mise en oeuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée en ce qui concerne les réseaux mondiaux, en veillant notamment:

- à encourager l'adoption de politiques en matière de vie privée, qu'elles soient mises en oeuvre par le recours à des mécanismes juridiques, administratifs, technologiques ou d'autorégulation;

- à encourager la notification en ligne aux utilisateurs des politiques en matière de vie privée;

- à garantir l'existence de mécanismes efficaces de mise en oeuvre permettant à la fois de régler les problèmes de non-respect des principes et des politiques de vie privée et de garantir l'accès à des moyens de réparation;

- à promouvoir l'éducation et la sensibilisation des utilisateurs aux problèmes de respect de la vie privée en ligne et aux moyens dont ils disposent pour protéger leur vie privée sur les réseaux mondiaux;

- à encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée; et

- à encourager l'utilisation de solutions contractuelles et le développement de solutions contractuelles types pour les flux transfrontières de données en ligne;

Qu'ils conviennent de faire le point des progrès accomplis pour se rapprocher des objectifs de la présente Déclaration, dans un délai de deux ans, et d'évaluer la nécessité d'actions supplémentaires pour assurer la protection des données de caractère personnel sur les réseaux mondiaux afin d'atteindre ces objectifs.

DÉCLARENT EN OUTRE QUE L'OCDE DEVRAIT

Aider les pays Membres à échanger des informations sur les méthodes efficaces pour protéger la vie privée sur les réseaux mondiaux et à faire part de leurs efforts et de leur expérience dans la réalisation des objectifs de la présente Déclaration;

Examiner les problèmes spécifiques soulevés par la mise en oeuvre des Lignes directrices de l'OCDE sur la protection de la vie privée en relation avec les réseaux mondiaux, et, après avoir collecté et diffusé des exemples d'expériences de mise en oeuvre des Lignes directrices, fournir aux pays Membres des orientations pratiques pour la mise en oeuvre des Lignes directrices dans l'environnement en ligne, en tenant compte des différentes approches à l'égard de la protection de la vie privée adoptées par les pays Membres et en s'inspirant de l'expérience des pays Membres et du secteur privé;

Coopérer avec l'industrie et les entreprises dans le cadre de leurs travaux en vue d'assurer la protection de la vie privée sur les réseaux mondiaux, ainsi qu'avec les organisations régionales et internationales compétentes;

Faire périodiquement le point des principales évolutions et questions dans le domaine de la protection de la vie privée eu égard aux objectifs de la présente Déclaration;

Prendre notamment en considération, dans le cadre de ses travaux futurs, les questions et les suggestions d'activités présentées dans le rapport qui accompagne cette Déclaration.

INVITENT

Les pays non membres à tenir compte de la présente Déclaration;

Les organisations internationales compétentes à prendre en considération la présente Déclaration lorsqu'elles élaborent ou modifient des conventions internationales, des Lignes directrices, des codes de conduite, des clauses contractuelles types, des technologies et des plates-formes interopérables pour la protection de la vie privée sur les réseaux mondiaux;

L'industrie et les entreprises à prendre en compte les objectifs de la présente Déclaration et à collaborer avec les gouvernements pour promouvoir ces objectifs en mettant en oeuvre des programmes visant la protection de la vie privée sur les réseaux mondiaux.

ANNEXE 2

DÉCLARATION SUR LA PROTECTION DES CONSOMMATEURS DANS LE CONTEXTE DU COMMERCE ELECTRONIQUE

qui a été formulée par les Ministres de l'OCDE
à la Conférence «Un monde sans frontières:
concrétiser le potentiel du commerce électronique mondial»
7-9 octobre 1998, Ottawa, Canada

Les Gouvernements des pays Membres de l'OCDE ¹²⁴⁾:

CONSIDÉRANT

que le volume comme la valeur des transactions des consommateurs sur les réseaux mondiaux augmentent de façon exponentielle;

que les réseaux mondiaux offrent aux consommateurs d'importants avantages, notamment une commodité et un accès à un large éventail de biens, de services et d'informations;

que ces avantages potentiels ne pourront se concrétiser si la confiance des consommateurs dans les activités commerciales menées sur les réseaux mondiaux est sapée par l'existence de comportements commerciaux frauduleux, fallacieux et déloyaux;

que la confiance dans les activités commerciales menées sur les réseaux mondiaux sera favorisée par des mécanismes transparents et efficaces de protection des consommateurs et que celle-ci est essentielle pour encourager la participation des consommateurs au marché électronique; et

¹²⁴⁾ incluant les Communautés européennes

qu'une coopération mondiale entre les gouvernements, les entreprises, les consommateurs et leurs représentants est une condition préalable indispensable pour parvenir à une protection des consommateurs efficace et prévisible dans le contexte du commerce électronique.

RECONNAISSANT

la nécessité pour les gouvernements, les entreprises, les consommateurs et leurs représentants de continuer d'oeuvrer ensemble à l'élaboration d'un cadre pour le commerce électronique mondial qui comporte une protection efficace pour les consommateurs et;

le dialogue permanent au sein de l'OCDE entre les gouvernements, les entreprises, les consommateurs et leurs représentants pour examiner les questions liées aux consommateurs et notamment les travaux en cours dans l'Organisation, par le biais de son Comité de la politique à l'égard des consommateurs, pour élaborer des Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique.

SE DÉCLARENT DÉTERMINÉS A

faire en sorte que les consommateurs qui prennent part au commerce électronique bénéficient d'un niveau transparent et efficace de protection pour les transactions électroniques, en s'attachant à:

- passer en revue et adapter les lois et pratiques, le cas échéant, en vue de prendre en compte les circonstances particulières du commerce électronique;
- soutenir et encourager la mise en place de mécanismes efficaces d'auto-régulation sous l'égide du secteur privé, qui prennent en compte les contributions des représentants des consommateurs et comportent des règles de fond spécifiques relatives aux mécanismes de règlement des litiges et de mise en application;
- encourager le développement technologique également en tant qu'instrument permettant de protéger les consommateurs;
- adopter des mesures en vue d'éduquer les utilisateurs, favoriser une prise de décision éclairée des consommateurs qui prennent part au commerce électronique, et sensibiliser davantage les entreprises au cadre général de protection des consommateurs qui s'applique à leurs activités en ligne; et
- sensibiliser davantage les autorités de justice et de police à la nécessité d'une coopération internationale efficace pour protéger les consommateurs et lutter contre les comportements commerciaux transfrontières frauduleux, fallacieux et déloyaux.

AFFIRMENT EN OUTRE QU'ILS SONT RESOLUS A:

élaborer des lignes directrices efficaces ayant pour objet de renforcer la confiance des consommateurs dans les transactions de commerce électronique tout en encourageant le développement du marché mondial; et

inviter instamment l'OCDE à achever ses travaux de rédaction de lignes directrices avant la fin de 1999, notamment en ce qui concerne les questions de protection des consommateurs telles que la divulgation intégrale et loyale des informations essentielles, la publicité, le traitement des plaintes, les voies de recours, la réparation ou autres questions pertinentes intéressant la protection des consommateurs.

ANNEXE 3

DECLARATION SUR L'AUTHENTIFICATION POUR
LE COMMERCE ELECTRONIQUE

qui a été formulée par les Ministres de l'OCDE
à la Conférence «Un monde sans frontières:
concrétiser le potentiel du commerce électronique mondial»
7-9 octobre 1998, Ottawa, Canada

Les Gouvernements des pays Membres de l'OCDE ¹²⁵⁾:

CONSIDERANT

les gains sociaux et économiques significatifs procurés par les technologies de l'information et des communications et par le commerce électronique;

le rôle éminent de l'industrie dans le développement des technologies de l'information et des communications et du commerce électronique;

le besoin du gouvernement et de l'industrie de stimuler la confiance des utilisateurs pour faciliter le développement du commerce électronique;

le développement rapide de technologies et mécanismes d'authentification et leur importance dans le contexte des technologies de l'information et des communications et du commerce électronique à l'échelle mondiale; et

l'impact potentiel que des solutions nationales diverses relatives à l'authentification électronique pourraient avoir sur le développement du commerce électronique mondial.

RECONNAISSANT

que des travaux sont en cours au niveau international pour faciliter les transactions électroniques transfrontières et l'utilisation des techniques et mécanismes d'authentification afin de stimuler le développement du commerce électronique à l'échelle mondiale;

que les parties contractantes pourront choisir les mécanismes adaptés à leurs besoins d'authentification dans le cadre de leur pratique du commerce électronique, notamment des technologies spécifiques de d'authentification électronique, des dispositifs contractuels ou d'autres moyens pour la validation des transactions électroniques, et qu'elles peuvent utiliser des moyens judiciaires ou autres de résolution de conflit pour prouver la validité de ces transactions;

que les pouvoirs publics peuvent contribuer à promouvoir le commerce électronique dans leur rôle d'utilisateurs de technologies, produits et services d'information et de communications, notamment des mécanismes électroniques d'authentification;

que les règles spécifiques de technologie ou de support pour l'enregistrement, le stockage ou la transmission de l'information (par exemple, certaines exigences fondées sur le papier) pourraient entraver le développement du commerce électronique et l'utilisation des mécanismes d'authentification électroniques;

¹²⁵⁾ incluant les Communautés européennes

que, le cas échéant, des normes et des codes de conduite émanant du secteur privé, plutôt qu'imposées par les gouvernements, peuvent fournir un outil efficace pour développer la confiance de l'utilisateur dans le commerce électronique mondial; et

qu'ils poursuivront le dialogue au sein de l'OCDE – impliquant les gouvernements, les entreprises et l'industrie, et les représentants des utilisateurs – pour discuter de manière plus approfondie les technologies et les divers modèles d'authentification destinés à faciliter le commerce électronique mondial qui sont actuellement utilisés ou en voie d'émergence dans les pays membres et, en particulier les travaux en cours dans l'Organisation, dans le cadre du Comité de la politique de l'information, de l'informatique et des communications (PIIC), pour faciliter l'échange d'information par la compilation d'un inventaire des approches de l'authentification et l'organisation d'ateliers mixtes OCDE-secteur privé dans l'année à venir.

LES MINISTRES SE DECLARENT RESOLUS A:

adopter une approche non discriminatoire à l'égard des mécanismes d'authentification électroniques émanant d'autres pays;

encourager les efforts pour développer des technologies et mécanismes d'authentification et faciliter l'utilisation de ces technologies et mécanismes pour le commerce électronique;

amender, le cas échéant, les exigences spécifiques sur la technologie ou les supports dans les lois actuelles ou les politiques susceptibles d'entraver l'utilisation des technologies de l'information et des communications et des mécanismes d'authentification électroniques, en tenant compte des dispositions appropriées de la Loi type sur le commerce électronique adoptée par la Commission des Nations Unies pour le droit commercial international (UNCITRAL) en 1996;

procéder à la mise en oeuvre des technologies d'authentification électronique pour améliorer la délivrance au public des services et programmes gouvernementaux; et

continuer d'oeuvrer à l'échelon international, conjointement avec les entreprises, l'industrie, et les représentants des utilisateurs, pour que les technologies et mécanismes d'authentification facilitent le commerce électronique mondial.